COMPOSITIO MATHEMATICA

Growth of Ш in towers for isogenous curves

Tim Dokchitser and Vladimir Dokchitser

Compositio Math. **151** (2015), 1981–2005.

doi:10.1112/S0010437X15007423

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY
150 YEARS

Compositio Math. 151 (2015) 1981–2005
doi:10.1112/S0010437X15007423

Growth of Ш in towers for isogenous curves

Tim Dokchitser and Vladimir Dokchitser

Abstract

We study the growth of Ш and p^∞-Selmer groups for isogenous abelian varieties in towers of number fields, with an emphasis on elliptic curves. The growth types are usually exponential, as in the 'positive μ-invariant' setting in the Iwasawa theory of elliptic curves. The towers we consider are p-adic and l-adic Lie extensions for $l \neq p$, in particular cyclotomic and other $\mathbb{Z}_l$-extensions.

1. Introduction

The algebraic side of the Iwasawa theory of elliptic curves is concerned with the study of the structure of Selmer groups in cyclotomic $\mathbb{Z}_p$-extensions of $\mathbb{Q}$, as well as other towers of number fields. The aim of the present paper is to systematically study the behaviour of Selmer groups for isogenous elliptic curves E and E' or abelian varieties. The isogeny makes it possible to bypass Iwasawa theory and, in particular, to avoid any assumptions on the reduction types. Moreover, it allows us to work with p^∞-Selmer groups in general l-adic towers, for both $l = p$ and $l \neq p$. For instance, we construct elliptic curves whose p-primary part of the Tate–Shafarevich group goes off to infinity in all l-cyclotomic extensions of $\mathbb{Q}$, in contrast to Washington's theorem which says that the p-part of the ideal class group is bounded in these extensions for $l \neq p$.

We show that in the nth layer of the p-cyclotomic tower of $\mathbb{Q}$, the quotient

$$|Ш_E[p^\infty]|/|Ш_{E'}[p^\infty]|$$

(if finite) is $p^{\mu p^n + O(1)}$, as though it came from an Iwasawa module with λ-invariant 0 and μ-invariant μ, except that μ may be fractional when E has potentially supersingular reduction at p. Our formula for μ is explicit and surprisingly simple, and there is similar behaviour in other p-adic and l-adic towers. It would be interesting to understand the structure theory of the associated Selmer groups that gives rise to such growth.

Our main results for $\mathbb{Z}_l$-extensions (Theorems 1.1 and 1.2) and general Lie groups (Theorem 1.3) are as follows.

Theorem 1.1. *Let $\bigcup_n \mathbb{Q}(l^n)$ be the l-cyclotomic tower, p a prime, and E and E' two isogenous elliptic curves over $\mathbb{Q}$. Then for all large enough n,*

$$\frac{|Ш^\circ_{E/\mathbb{Q}(l^n)}[p^\infty]|}{|Ш^\circ_{E'/\mathbb{Q}(l^n)}[p^\infty]|} = p^{\mu l^n + \nu + \epsilon(n)}$$

for some $\nu \in \mathbb{Z}$, some $|\epsilon(n)| \leqslant 8\frac{1}{2}$ and $\mu \in \frac{1}{12}\mathbb{Z}$ given by

Received 10 June 2014, accepted in final form 24 February 2015, published online 30 June 2015.
2010 Mathematics Subject Classification 11G40, 11G05 (primary), 11G10, 11G07, 11R23, 11D68 (secondary).
Keywords: elliptic curves, Selmer group, Tate–Shafarevich group, p-adic Lie extensions, isogeny, Iwasawa theory, μ-invariant, abelian varieties.

$$\mu = \mathrm{ord}_p \frac{\Omega_{E'}}{\Omega_E} + \begin{cases} 0 & \text{if } l \neq p \text{ or } \mathrm{ord}_p(j_E) < 0, \\ \frac{1}{12}\mathrm{ord}_p\left(\frac{\Delta_{E'}}{\Delta_E}\right) & \text{if } l = p \text{ and } \mathrm{ord}_p(j_E) \geqslant 0. \end{cases}$$

If $l \neq p$ or l does not divide the degree of the isogeny $E \to E'$, then $\epsilon(n) = 0$.

Here and throughout the paper, $\mathbb{Q}(l^n)$ denotes the degree-l^n extension of $\mathbb{Q}$ in the cyclotomic $\mathbb{Z}_l$-extension. We write Δ_E and $\Delta_{E'}$ for the minimal discriminants[1] of the two curves, j_E and $j_{E'}$ for the j-invariants, Ω_E and $\Omega_{E'}$ for the Birch–Swinnerton-Dyer periods (see § 2), and $Ш^\circ$ for the Tate–Shafarevich group Ш modulo its divisible part $Ш^{\mathrm{div}}$. We also write Sel_{p^∞} for the p^∞-Selmer group, $\mathrm{Sel}_{p^\infty}^{\mathrm{div}}$ for its divisible part, rk_p for its $\mathbb{Z}_p$-corank,[2] c_v for the Tamagawa number at v, and $f_{K_v/\mathbb{Q}_p}$ for the residue degree of $K_v/\mathbb{Q}_p$. The big-O notation refers to the parameter n.

Theorem 1.2. *Let K be a number field, p a prime number, and $K_\infty = \bigcup_n K_n$ a $\mathbb{Z}_l$-extension of K, with $[K_n : K] = l^n$. Let $\phi : E \to E'$ be an isogeny of elliptic curves over K, with dual isogeny ϕ^t. Then*

$$\frac{|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(E/K_n)[\phi]|}{|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(E'/K_n)[\phi^t]|}\frac{|Ш^\circ_{E/K_n}[p^\infty]|}{|Ш^\circ_{E'/K_n}[p^\infty]|} = p^{\mu l^n + O(1)}, \quad \mu = \mathrm{ord}_p\left(\frac{\Omega_{E'/K}}{\Omega_{E/K}}\right) + \sum_v \mu_v,$$

where the sum is taken over primes v of bad reduction for E/K and

$$\mu_v = \begin{cases} \mathrm{ord}_p \frac{c_v(E'/K)}{c_v(E/K)} & \text{if } v \text{ is totally split in } K_\infty/K, \\ \frac{f_{K_v/\mathbb{Q}_p}}{12}\mathrm{ord}_v\left(\frac{\Delta_{E'}}{\Delta_E}\right) & \text{if } l = p,\ v \mid p \text{ is ramified in } K_\infty/K \text{ and } \mathrm{ord}_v\, j_E \geqslant 0, \\ 0 & \text{otherwise.} \end{cases}$$

If $\mathrm{rk}_p\, E/K_n$ is bounded, then $|Ш^\circ_{E/K_n}[p^\infty]|/|Ш^\circ_{E'/K_n}[p^\infty]| = p^{\mu l^n + O(1)}$ as well.

Theorem 1.3. *Suppose that K is a number field and K_∞/K is a Galois extension whose Galois group is a d-dimensional l-adic Lie group; write K_n/K for its nth layer in the natural l-adic Lie filtration. Let p be a prime number and $\phi : A \to A'$ an isogeny of abelian varieties over K, with dual $\phi^t : A'^t \to A^t$.*

(i) *If A is an elliptic curve, then there is $\mu \in \mathbb{Q}$ such that*

$$\frac{|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K_n)[\phi]|}{|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A'/K_n)[\phi^t]|}\frac{|Ш^\circ_{A/K_n}[p^\infty]|}{|Ш^\circ_{A'/K_n}[p^\infty]|} = p^{\mu l^{dn} + O(l^{(d-1)n})}.$$

(ii) *If A and A' are either semistable abelian varieties or elliptic curves that do not have additive potentially supersingular reduction at primes $v \mid p$ that are infinitely ramified in K_∞/K, then there are constants $\mu_1, \ldots, \mu_{d-1} \in \mathbb{Q}$ such that for all sufficiently large n,*

$$\frac{|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K_n)[\phi]|}{|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A'^t/K_n)[\phi^t]|}\frac{|Ш^\circ_{A/K_n}[p^\infty]|}{|Ш^\circ_{A'/K_n}[p^\infty]|} = p^{\mu l^{dn} + \mu_1 l^{(d-1)n} + \cdots + \mu_{d-1} l^n + O(1)}.$$

If $A(K_n)[p^\infty]$ is bounded, $O(1)$ may be replaced by a constant $\mu_d \in \mathbb{Q}$.

(iii) *If $\mathrm{rk}_p\, A/K_n$ is $O(l^{(d-1)n})$ in* (i) *or $O(1)$ in* (ii)*, then all the conclusions of* (i) *or* (ii)*, respectively, hold for $|Ш^\circ_{A/K_n}[p^\infty]|/|Ш^\circ_{A'/K_n}[p^\infty]|$ as well.*

[1] If the base field is not $\mathbb{Q}$, there may be no global minimal model. We then regard Δ_E and $\Delta_{E'}$ as ideals that have minimal valuation at every prime.

[2] Thus, $\mathrm{rk}_p\, A/K = \mathrm{rk}\, A/K + t$ if $Ш^{\mathrm{div}}_{A/K} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^t$. Of course, conjecturally, $t = 0$, $Ш = Ш^\circ$ and $\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K) \cong A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. In any case, $Ш^\circ$ is a torsion abelian group all of whose p-primary parts are finite.

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

Remarks 1.4. (1) If $p \nmid \deg\phi$, then the p^∞-Selmer groups and the p-part of Ш cannot have ϕ-torsion, so the corresponding quotients in Theorems 1.1–1.3 are trivial. The results can be reduced to those for isogenies of p-power degree.

(2) In Theorems 1.1 and 1.2, the quotient $\Omega_{E'}/\Omega_E$ is a rational number (Lemma 2.3). For p-isogenous curves over $\mathbb{Q}$ it is 1 or $p^{\pm 1}$; see [DD15, Theorem 8.2]. The term $\frac{1}{12}\mathrm{ord}_p(\Delta_{E'}/\Delta_E)$ is 0 unless E has additive potentially supersingular reduction at p; see [DD15, Table 1]. In this exceptional case, μ does not have to be an integer; see Example 1.6.

(3) Suppose that $\mathrm{Gal}(K_\infty/K) = \Gamma \cong \mathbb{Z}_p$. If the dual p^∞-Selmer group of E/K_∞ is a torsion $\mathbb{Z}_p[[\Gamma]]$-module, then the invariant μ of Theorem 1.2 is $\mu(E)-\mu(E')$, the difference of the classical μ-invariants of the two Selmer groups over K_∞. In this setting, Theorem 1.2 is equivalent to a theorem of Schneider (for odd p); see [Sch87] and [Per87, Appendix].

(4) Suppose that $E/\mathbb{Q}$ has good ordinary reduction at p. Then the dual p^∞-Selmer group of E over the p-cyclotomic extension over $\mathbb{Q}$ is a torsion Iwasawa module, by Kato's theorem [Kat04]. A conjecture of Greenberg [Gre99, Conjecture 1.11] asserts that the isogeny class of E contains a curve of μ-invariant 0. Granting the conjecture, Theorem 1.1 implies that:

(a) in the isogeny class of $E/\mathbb{Q}$, the curve E_m with the largest period Ω_{E_m} has μ-invariant 0 at all primes of good ordinary reduction;
(b) E has μ-invariant $\mathrm{ord}_p(\Omega_{E_m}/\Omega_E)$ at p.

Thus, the theorem provides a conjectural formula for the μ-invariant. We note here that Greenberg's conjecture is known not to hold in general over number fields; see [Dri03].

(5) Greenberg (see [Gre01, Exercises 4.3–4.5]) has observed that if $\phi : E \to E'$ is a p-isogeny over K whose kernel is μ_p, then the map

$$K^\times/K^{\times p} \cong H^1(\mathrm{Gal}(\bar{K}/K), \mu_p) \longrightarrow H^1(\mathrm{Gal}(\bar{K}/K), E[p])$$

induced by the inclusion $\mu_p \subset E[p]$ provides a way to construct classes in the p-Selmer group of E. The units of K contribute to the Selmer group, and the rank of the unit group is roughly $[K:\mathbb{Q}]$. In particular, one can exhibit μ-like growth of $\mathrm{Sel}_p(E)$ in towers K_n/K. It would be interesting to similarly explain the Selmer growth in Theorems 1.1–1.3 for p-power isogenies with arbitrary kernels.

(6) By a theorem of Washington [Was78], for $p \neq l$ the p-part of the ideal class group is bounded in the l-cyclotomic tower. Theorem 1.2 provides examples of elliptic curves over $\mathbb{Q}$ for which the analogous statement for the Tate–Shafarevich group fails; see, for instance, Example 1.5.

In the opposite direction, Lamplugh [Lam] has recently proven the following analogue of the theorem of Washington for elliptic curves $E/\mathbb{Q}$ with complex multiplication by the ring of integers of an imaginary quadratic field K. Let $p > 3$ and $l > 3$ be distinct primes of good reduction of E that split in $K/\mathbb{Q}$. Lamplugh proved that if K_n is the nth layer of the unique $\mathbb{Z}_l$-extension of K unramified outside one of the factors of l in K, then the p^∞-Selmer group of E over K_n stabilises as $n \to \infty$.

(7) The constants μ and $\mu_1, \ldots, \mu_d$ in Theorem 1.3 can be made explicit, as in Theorem 1.2. Following the proof of Theorem 8.7, this requires knowledge of the decomposition and inertia groups at bad primes; the other ingredients are computed in Proposition 8.5.

Example 1.5 (Ordinary reduction). Let us show that the curves $11a1$ and $11a2$ have unbounded 5-primary part of Ш in the cyclotomic $\mathbb{Z}_l$-extension of $\mathbb{Q}$ for every prime l. There are 5-isogenies

$$11a2 \longrightarrow 11a1 \longrightarrow 11a3,$$

and $\Omega_{11a3} = 5\Omega_{11a1} = 25\Omega_{11a2} = 6.34604\ldots$. So, by Theorem 1.1, for every l there exist $\nu_l, \nu_l' \in \mathbb{Z}$ such that

$$|\text{Ш}_{11a2/\mathbb{Q}(l^n)}[5^\infty]| \geqslant 25^{l^n-\nu_l}, \quad |\text{Ш}_{11a1/\mathbb{Q}(l^n)}[5^\infty]| \geqslant 5^{l^n-\nu_l'}.$$

A standard computation with cyclotomic Euler characteristics (as in [DD06, § 3.11], for example) shows that for every ordinary prime l for which $a_l \neq 1$ (e.g. $l = 3, 7, 13, 17, \ldots$), the curves have rank 0 over $\mathbb{Q}(l^n)$ for all $n \geqslant 1$. For such primes, ν_l and ν_l' can be taken to be 1 and the number of primes above 11 in $\bigcup_n \mathbb{Q}(l^n)$, respectively.[3] For $l = 5$, these bounds are exact, as $\text{Ш}_{11a3/\mathbb{Q}(5^n)}$ is known to have trivial 5-primary part for all $n \geqslant 1$.

Example 1.6 (Potentially supersingular reduction). Let $E/\mathbb{Q}$ be an elliptic curve with good supersingular reduction at p, and let $K_n = \mathbb{Q}(p^n)$, the nth layer in the p-cyclotomic tower. By a theorem of Kurihara [Kur02], under suitable hypotheses,

$$|\text{Ш}_{E/K_n}[p^\infty]| = p^{\lfloor \mu p^n - 1/2 \rfloor}, \quad \mu = \frac{p}{p^2-1}.$$

Note that such curves cannot have a p-isogeny, by a result of Serre [Ser72, Proposition 12]. In contrast, elliptic curves over $\mathbb{Q}$ with additive potentially supersingular reduction at p can have a p-isogeny, and there are examples for which

$$|\text{Ш}_{E/K_n}[p^\infty]| \geqslant p^{\mu p^n + \nu}$$

with $\mu > 1$. For instance, there is a 9-isogeny $\phi : 54a2 \to 54a3$. These curves have potentially supersingular reduction at $p = 3$, and

$$\Omega_{54a3} = 9\Omega_{54a2}, \quad \Delta_{54a2} = -2^9 3^{11}, \quad \Delta_{54a3} = -2 \cdot 3^3.$$

By Theorem 1.1, there is a constant ν such that for all large enough n,

$$|\text{Ш}_{54a2/K_n}[3^\infty]| \geqslant \frac{|\text{Ш}_{54a2/K_n}[3^\infty]|}{|\text{Ш}_{54a3/K_n}[3^\infty]|} = 3^{3^n\mu+\nu}, \quad \mu = 2 - \frac{11-3}{12} = \frac{4}{3}.$$

Example 1.7 (False Tate curve tower). To illustrate Theorem 1.3 for a higher-dimensional l-adic Lie group, let $K_n = \mathbb{Q}(\zeta_{3^n}, \sqrt[3^n]{7})$, a 'false Tate curve tower' in the terminology of [HV03, DD06]. Let $E = 11a1$ and $E' = 11a3$, as in Example 1.5. We find (see Example 3.3) that either $\text{Ш}_{E/K_n}[5^\infty]$ is infinite or

$$\frac{|\text{Ш}_{E/K_n}[5^\infty]|}{|\text{Ш}_{E'/K_n}[5^\infty]|} = 5^{3^{2n-1}-3^n}.$$

Example 1.8. Let K_∞ be the unique $\mathbb{Z}_5^2$-extension of $\mathbb{Q}(i)$ and let K_n be its nth layer; thus $\text{Gal}(K_n/\mathbb{Q}) \cong C_{5^n} \times D_{2\cdot 5^n}$. If we take the 5-isogenous curves $E = 75a1$ and $E' = 75a2$ over $\mathbb{Q}$, with additive potentially supersingular reduction at 5, we find that (see Example 3.4)

$$\frac{|\text{Sel}^{\text{div}}_{5^\infty}(E/K_n)[\phi]|}{|\text{Sel}^{\text{div}}_{5^\infty}(E'/K_n)[\phi^t]|} \frac{|\text{Ш}^\circ_{E/K_n}[5^\infty]|}{|\text{Ш}^\circ_{E'/K_n}[5^\infty]|} = 5^{\mu 5^{2n} + \mu_1(n) 5^n + \mu_2(n)}$$

[3] So ν_l' is almost always 1 as well; for $l < 10^7$ the only exception is $l = 71$.

with

$$\mu = -\tfrac{1}{3}, \quad \mu_1(n) = 1 - \tfrac{2}{3}(-1)^n, \quad \mu_2(n) = 0.$$

So the assumption in Theorem 1.3(ii) that E does not have potentially supersingular reduction cannot be removed, as the μ_i may fluctuate with n.

Example 1.9. As opposed to the cyclotomic extensions, for general $\mathbb{Z}_l$-extensions of number fields there is an extra term in μ coming from the Tamagawa numbers (compare Theorem 1.2 with Theorem 1.1). For example, consider the 5-isogeny $11a1 \to 11a3$, as in Example 1.5, in the 5-anticyclotomic tower K_∞ of $K = \mathbb{Q}(i)$. Because 11 is inert in $\mathbb{Q}(i)$ and so totally split in K_∞/K, there is a μ-contribution from the Tamagawa numbers (5 and 1) in this $\mathbb{Z}_5$-extension, but not in the cyclotomic one.

Remark 1.10 (CM curves with $\mu > 0$). If K_∞/K is a $\mathbb{Z}_p$-extension and $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is cotorsion over the Iwasawa algebra of $\mathrm{Gal}(K_\infty/K)$, then it has a well-defined μ-invariant as in classical Iwasawa theory. Theorem 1.2 gives a formula for its change under isogenies in terms of elementary invariants, and allows us to generate examples with positive μ-invariant.

Consider, for instance, elliptic curves with complex multiplication and good ordinary reduction at p. Such examples over $\mathbb{Q}$ with a p-isogeny are almost non-existent: there are 13 CM j-invariants over $\mathbb{Q}$, and there is only one with a p-isogeny that admits good reduction at p. It is $j = -3^3 5^3$ (CM by $\mathbb{Z}[(1+\sqrt{-7})/2]$), 2-isogenous to $j = 3^3 5^3 17^3$ (CM by $\mathbb{Z}[\sqrt{-7}]$). (This is easy to check from the table of CM j-invariants [Sil94, Appendix A] and by computing the isogenous curves, e.g. using Magma [BCP97].) The simplest example with these j-invariants is

$$\phi : 49a1 \longrightarrow 49a2.$$

Here $\Omega_{49a1}/\Omega_{49a2} = 2$, and so $49a2$ does have positive μ-invariant for $p = 2$ as well as unbounded 2-part of Ш in every cyclotomic $\mathbb{Z}_l$-extension of $\mathbb{Q}$, by Theorem 1.1. Assuming Greenberg's conjecture (Remark 1.4(4)), the curve $49a2$ and $p = 2$ is the unique example (up to quadratic twists) of a good ordinary CM curve over $\mathbb{Q}$ with positive μ-invariant.

Over larger number fields, other examples are easy to construct. For instance, the curve

$$E : y^2 = x^3 - 24z^7\sqrt{z+3}\,x^2 + zx, \quad z = \frac{\sqrt{5}-1}{2}$$

is defined over $K = \mathbb{Q}(\zeta_{20})^+ = \mathbb{Q}(\sqrt{z+3})$ and has CM by $\mathbb{Z} + 5i\mathbb{Z}$. It has good ordinary reduction at the prime above 5, and is 5-isogenous to $y^2 = x^3 + zx$. Upon computing the periods and applying Theorem 1.2, we find that it should have positive μ-invariant both over the $\mathbb{Z}_5$-cyclotomic extension of K and over every $\mathbb{Z}_5$-extension of $K(i) = \mathbb{Q}(\zeta_{20})$.

Let F_∞ be the composite of all $\mathbb{Z}_5$-extensions of $K(i)$, so that $G = \mathrm{Gal}(F_\infty/K) \cong \mathbb{Z}_5^5$. The 5^∞-Selmer group of E over F_∞ is conjectured to satisfy the $\mathcal{M}_H(G)$-conjecture of non-commutative Iwasawa theory [CFKSV05]. As John Coates remarked to us, this example provides evidence for the conjecture as follows. Similar arguments to those given in [CS12] would show that the $\mathcal{M}_H(G)$-conjecture implies that the μ_G-invariant of the Selmer group over F_∞ has to be equal to the usual μ-invariant of the Selmer group over the cyclotomic $\mathbb{Z}_5$-extension of $K(i)$, which we have shown to be non-zero. Thus, granted the $\mathcal{M}_H(G)$-conjecture, it would follow that the μ_G-invariant of the Selmer group over F_∞ has to be positive, and then an easy further argument shows that the μ-invariant over every $\mathbb{Z}_5$-extension of $K(i)$ would also be positive, in accord with what we have proven.

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

Brief overview of the paper. To control the change of Selmer groups, we invoke the theorem by Cassels and Tate [Cas65, Tat65/66] on the invariance of the Birch–Swinnerton-Dyer conjecture under isogeny. This is recalled in Theorem 3.1 in § 3, after we introduce a convenient choice of periods in § 2. Most of the rest of the paper studies how the terms of the Birch–Swinnerton-Dyer formula behave in towers of local fields and number fields: minimal differentials in § 4, Tamagawa numbers in § 5, torsion in § 6, and the divisible part of Selmer in § 7. At the end of § 3 we also give some examples of how this procedure works. Theorems 1.1–1.3 are proved in § 8. In §§ 4 and 5 we rely on the results of [DD15] that describe how local invariants of elliptic curves change under isogeny.

The Appendix concerns the behaviour of conductors of elliptic curves and Galois representations in field extensions. There is no assumption on the existence of an isogeny here, and the results may be of independent interest.

Notation. We write E and E' for elliptic curves and A and A' for abelian varieties. We usually have an isogeny $E \to E'$ or $A \to A'$, denoted by ϕ. Its dual $E' \to E$ or $(A')^t \to A^t$ is denoted by ϕ^t. Number fields are denoted by $K, F, \ldots$, and l-adic fields (finite extensions of $\mathbb{Q}_l$) are denoted by $\mathcal{K}, \mathcal{F}, \ldots$. We also use the following notation:

$\lvert\cdot\rvert_v$	normalised absolute value at a prime v;
$v(\cdot)$, $\mathrm{ord}_v(\cdot)$	normalised valuation in a local field or at v;
j_E	j-invariant of an elliptic curve E;
$\Delta_E, \Delta_{E/K}$	minimal discriminant of an elliptic curve over K;
δ, δ'	$v(\Delta_{E/\mathcal{K}}), v(\Delta_{E'/\mathcal{K}})$ when $\mathcal{K}$ is local;
$f_{E/\mathcal{K}}$	conductor exponent of $E/\mathcal{K}$ when $\mathcal{K}$ is local;
$\mathrm{Om}_\phi(\mathcal{F})$	see Definition 4.1;
$\omega_v^{\min} = \omega_{A,v}^{\min}$	Néron minimal exterior form of an abelian variety at a prime v (minimal differential for an elliptic curve);
$c_{A/K}, c_v(A/K)$	Tamagawa number over a local/global field at v;
Ω, Ω^*	infinite periods (see Definition 2.1);
$Ш, Ш^{\mathrm{div}}, Ш^\circ$	Tate–Shafarevich group, its divisible part, $Ш^\circ = Ш/Ш^{\mathrm{div}}$;
$\mathrm{Sel}_{p^\infty}(A/K)$	$\varinjlim \mathrm{Sel}_{p^n}(A/K)$, the p-infinity Selmer group;
$\mathrm{rk}_p(A/K)$	$\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(A/K)$;
$\mathbb{Q}(l^n)$	the nth layer of the cyclotomic $\mathbb{Z}_l$-extension of $\mathbb{Q}$, i.e. the unique totally real degree-l^n subfield of $\mathbb{Q}(\zeta_{l^{n+2}})$;
$X[\phi], X[p^\infty]$	ϕ-torsion, p-primary component of an abelian group X;
$\lfloor\cdot\rfloor, \{\cdot\}$	integer part (floor) and fractional part $\{x\} = x - \lfloor x \rfloor$.

Any two non-zero invariant exterior forms ω_1 and ω_2 on an abelian variety A/K are multiples of one another, i.e. $\omega_1 = \alpha\omega_2$ with $\alpha \in K$. We will write ω_1/ω_2 for the scaling factor α.

When $\mathcal{K}$ is an l-adic field, recall that an elliptic curve $E/\mathcal{K}$ has additive reduction if and only if it has conductor exponent $f_{E/\mathcal{K}} \geqslant 2$, and that $f_{E/\mathcal{K}} = 2$ if and only if the ℓ-adic Tate module of E is tamely ramified for some (any) $\ell \neq l$. We call the reduction *tame* in the latter case, and *wild* if $f_{E/\mathcal{K}} > 2$. If $l \geqslant 5$, the reduction is always tame. We remind the reader that $E/\mathcal{K}$ has potentially good reduction if $v(j_E) \geqslant 0$ and potentially multiplicative reduction if $v(j_E) < 0$.

Finally, an *l-adic Lie group* G is a closed subgroup $\mathrm{GL}_k(\mathbb{Z}_l)$ for some k; it has a natural filtration by open subgroups, the kernels of the reduction maps mod l^n.

We use Cremona's notation (such as $11a1$) for elliptic curves over $\mathbb{Q}$.

2. Periods

We introduce a convenient form of periods of abelian varieties over number fields, which are model-independent and well-suited for the Birch–Swinnerton-Dyer conjecture.

DEFINITION 2.1. An abelian variety A/K has a non-zero invariant exterior form ω, unique up to K-multiples. If $K=\mathbb{C}$, we define the *local period*

$$\Omega_{A/\mathbb{C},\omega} = \int_{A(\mathbb{C})} 2^{\dim A}|\omega \wedge \overline{\omega}|.$$

If $K=\mathbb{R}$, define

$$\Omega_{A/\mathbb{R},\omega} = \int_{A(\mathbb{R})} |\omega| \quad \text{and} \quad \Omega^*_{A/\mathbb{R}} = \frac{\Omega_{A/\mathbb{C},\omega}}{\Omega^2_{A/\mathbb{R},\omega}}.$$

If K is a number field, define the *global period*

$$\Omega_{A/K} = \prod_{v\nmid\infty} |\omega/\omega_v^{\min}|_v \prod_{v|\infty} \Omega_{A/K_v,\omega}.$$

Here v runs through places of K, and the term at v in the first product is the normalised v-adic absolute value of the quotient of ω by the Néron minimal form at v.

Remark 2.2. Note that both Ω^*_{A/K_v} and $\Omega_{A/K}$ are independent of the choice of ω, by the product formula for the second one.

An elliptic curve $E/\mathbb{Q}$ can be put in minimal Weierstrass form, with the global minimal differential $\omega = dx/(2y+a_1x+a_3)$. Then $\Omega_{E/\mathbb{Q}} = \Omega_{E/\mathbb{R},\omega}$, which is the traditional real period Ω_+ or $2\Omega_+$, depending on whether or not $E(\mathbb{R})$ is connected. If $E(\mathbb{C}) = \mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}$ under the usual complex uniformisation, then $\Omega^*_{E/\mathbb{R}} = \operatorname{Im}\tau$.

LEMMA 2.3. *Let $\phi: A \to A'$ be an isogeny of abelian varieties over a number field K. Then both $\Omega_{A'/K}/\Omega_{A/K}$ and, for real places v, $\Omega^*_{A'/K_v}/\Omega^*_{A/K_v}$ are positive rational numbers. They have trivial p-adic valuation for all $p \nmid \deg\phi$.*

Proof. Fix a non-zero invariant exterior form ω' on A', and set $\omega = \phi^*\omega'$. For $v\,|\,\infty$,

$$\frac{\Omega_{A'/K_v,\omega'}}{\Omega_{A/K_v,\omega}} = \frac{|\operatorname{coker}\phi : A(K_v) \to A'(K_v)|}{|\ker\phi : A(K_v) \to A'(K_v)|}.$$

This is a positive rational, and considering the conjugate isogeny $\phi': A' \to A$ (so that $\phi'\circ\phi$ and $\phi\circ\phi'$ are the multiplication-by-$\deg\phi$ maps), we see that the only prime factors of $|\ker|$ and $|\operatorname{coker}|$ are those dividing $\deg\phi$. The claim for Ω^* now follows.

As for the global periods,

$$\frac{\Omega_{A'/K}}{\Omega_{A/K}} = \prod_{v\nmid\infty} \frac{|\omega'/\omega^{\min}_{A',v}|_v}{|\omega/\omega^{\min}_{A,v}|_v} \prod_{v|\infty} \frac{\Omega_{A'/K_v,\omega'}}{\Omega_{A/K_v,\omega}}$$

is a positive rational. If $v \nmid \deg\phi$, then $\phi^*(\omega^{\min}_{A',v})$ is a unit multiple of $\omega^{\min}_{A,v}$, and so $|\omega'/\omega^{\min}_{A',v}|_v/|\omega/\omega^{\min}_{A,v}|_v = 1$. Thus $\Omega_{A'/K}/\Omega_{A/K}$ has trivial p-adic valuation at primes $p \nmid \deg\phi$. $\square$

Lemma 2.4. *Let A be an abelian variety over a number field K, and let F/K be a finite extension. Then*

$$\Omega_{A/F}=\Omega_{A/K}^{[F:K]}\prod_{v\ \textit{real}}(\Omega^*_{A/K_v})^{\#\{w|v\ \textit{complex}\}}\prod_{v,w|v}\left|\frac{\omega_v^{\min}}{\omega_w^{\min}}\right|_w,$$

where v runs over places of K and w over places of F above v.

Proof. Choose an invariant exterior form ω for A/K. We compute the terms in $\Omega_{A/F}$ using ω.

Let v be a place of K. If v is complex, then $\prod_{w|v}\Omega_{A/F_w,\omega}=\Omega_{A/K_v,\omega}^{[F:K]}$. If v is real, then, writing Σ_+ and Σ_- for the sets of real and complex places $w\,|\,v$ in F, we have

$$\prod_{w|v}\Omega_{A/F_w,\omega}=\prod_{w\in\Sigma_+}\Omega_{A/K_v,\omega}\prod_{w\in\Sigma_-}\Omega^2_{A/K_v,\omega}\Omega^*_{A/K_v}=\Omega_{A/K_v,\omega}^{[F:K]}(\Omega^*_{A/K_v})^{|\Sigma_-|}.$$

If $v\nmid\infty$, then

$$\prod_{w|v}\left|\frac{\omega}{\omega_w^{\min}}\right|_w=\prod_{w|v}\left|\frac{\omega}{\omega_v^{\min}}\right|_w\left|\frac{\omega_v^{\min}}{\omega_w^{\min}}\right|_w=\left|\frac{\omega}{\omega_v^{\min}}\right|_v^{[F:K]}\prod_{w|v}\left|\frac{\omega_v^{\min}}{\omega_w^{\min}}\right|_w.$$

Multiplying the terms over all places v of K gives the claim. □

Remark 2.5. For elliptic curves, the term $\omega_v^{\min}/\omega_w^{\min}$ relates to the behaviour of the minimal discriminant of E in F_w/K_v (cf. [Sil86, Table III.1.2]),

$$\mathrm{ord}_w\left(\frac{\omega_w^{\min}}{\omega_v^{\min}}\right)=\frac{1}{12}\,\mathrm{ord}_w\left(\frac{\Delta_{E/K}}{\Delta_{E/F}}\right).$$

3. BSD invariance under isogeny

We now state a version of the invariance of the Birch–Swinnerton-Dyer conjecture under isogeny for Selmer groups (see p. 1986 for the notation).

Theorem 3.1. *Let $\phi:A\to A'$ be a isogeny of abelian varieties over a number field K, and let $\phi^t:A'^t\to A^t$ be the dual isogeny. If the degree of ϕ is a power of p, then*

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A'^t/K)[\phi^t]|}\frac{|\text{Ш}^\circ_{A/K}[p^\infty]|}{|\text{Ш}^\circ_{A'/K}[p^\infty]|}=\frac{|A(K)[p^\infty]|\,|A^t(K)[p^\infty]|}{|A'(K)[p^\infty]|\,|A'^t(K)[p^\infty]|}\frac{\Omega_{A'/K}}{\Omega_{A/K}}\prod_{v\nmid\infty}\frac{c_v(A'/K)}{c_v(A/K)}.$$

Otherwise, the left-hand side and right-hand side have the same p-part.

Proof. This is essentially [DD10, Theorem 4.3], which says that

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A'^t/K)[\phi^t]|}\prod_{p|\deg\phi}\frac{|\text{Ш}^\circ_{A/K}[p^\infty]|}{|\text{Ш}^\circ_{A'/K}[p^\infty]|}=\frac{|A(K)_{\mathrm{tors}}|\,|A^t(K)_{\mathrm{tors}}|}{|A'(K)_{\mathrm{tors}}|\,|A'^t(K)_{\mathrm{tors}}|}\frac{\Omega_{A'/K}}{\Omega_{A/K}}\prod_{v\nmid\infty}\frac{c_v(A'/K)}{c_v(A/K)}.$$

The term $Q(\phi)$ in [DD10] is exactly $\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K)[\phi]$. □

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

COROLLARY 3.2. *Let $\phi : A \to A'$ be an isogeny of abelian varieties over a number field K with dual $\phi^t : A'^t \to A^t$, and let F/K be a finite extension. If the degree of ϕ is a power of p, then*

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/F)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A'^t/F)[\phi^t]|}\frac{|Ш^\circ_{A/F}[p^\infty]|}{|Ш^\circ_{A'/F}[p^\infty]|} = \frac{|A(F)[p^\infty]|\,|A^t(F)[p^\infty]|}{|A'(F)[p^\infty]|\,|A'^t(F)[p^\infty]|}\left(\frac{\Omega_{A'/K}}{\Omega_{A/K}}\right)^{[F:K]}$$
$$\times\prod_{v\ real}\left(\frac{\Omega^*_{A'/K_v}}{\Omega^*_{A/K_v}}\right)^{\#\{w|v\ complex\}}\prod_{v\nmid\infty}\frac{c_v(A'/F)}{c_v(A/F)}\prod_{v,w|v}\left|\frac{\omega^{\min}_{A',v}/\omega^{\min}_{A',w}}{\omega^{\min}_{A,v}/\omega^{\min}_{A,w}}\right|_w,$$

where v ranges over places of K and the $w\,|\,v$ are places of F. If ϕ has arbitrary degree, then the left-hand side and right-hand side have the same p-part.

Proof. Combine Theorem 3.1 with Lemma 2.4. □

Corollary 3.2 is our main tool for studying the Selmer growth in towers in § 8. As we now illustrate, it already enables us to construct explicit examples of interesting growth of Selmer and Ш. The general behaviour of the Tamagawa number quotient will be discussed in § 5, the torsion quotient in § 6, and the contribution from exterior forms in § 4, under the name of $\mathrm{Om}_\phi(F_w)$.

Example 3.3. Let $K_n = \mathbb{Q}(\zeta_{3^n}, \sqrt[3^n]{7})$, a 'false Tate curve tower' in the terminology of [HV03, DD06], and let $\phi : E = 11a1 \to E' = 11a3$ be the 5-isogeny as in Example 1.5. A result of Hachimori and Matsuno [HM99, Theorem 3.1] and a cyclotomic Euler characteristic computation as in [DD06, § 3.11] show that $\mathrm{rk}\,E/K_n = \mathrm{rk}_3\,E/K_n = 0$ for all $n \geqslant 1$. Therefore

$$\mathrm{Sel}_{5^\infty}(E/K_n) = Ш_{E/K_n}[5^\infty],$$

and similarly for E'.

The periods of the two curves are

$$\Omega_{E/\mathbb{Q}} = 1.2692\ldots = \tfrac{1}{5}\Omega_{E'/\mathbb{Q}},\quad \Omega^*_{E/\mathbb{R}} = 1.1493\ldots = 5\Omega^*_{E'/\mathbb{R}},$$

and both curves have torsion of size 5 over all K_n. Applying Corollary 3.2, we find that either $Ш_{E/K_n}[5^\infty]$ is infinite for some n, or

$$\frac{|Ш_{E/K_n}[5^\infty]|}{|Ш_{E'/K_n}[5^\infty]|} = \frac{5^2}{5^2}\cdot\left(\frac{\Omega_{E'/\mathbb{Q}}}{\Omega_{E/\mathbb{Q}}}\right)^{2\cdot 3^{2n-1}}\cdot\left(\frac{\Omega^*_{E'/\mathbb{R}}}{\Omega^*_{E/\mathbb{R}}}\right)^{3^{2n-1}}\cdot\prod_{v|11}\frac{c_v(E'/K_n)}{c_v(E/K_n)}\cdot 1$$
$$= \frac{5^{2\cdot 3^{2n-1}}}{5^{3^{2n-1}}\cdot 5^{3^n}} = 5^{3^{2n-1}-3^n}.$$

Example 3.4 (Fluctuation in Selmer growth). In the previous example, the quotient of the Tate–Shafarevich groups grew like $5^{3^{2n-1}-3^n}$. Theorem 1.3 shows that such growth of the form $p^{\text{polynomial in } l^n}$ is a general phenomenon. However, the assumption on primes of additive potentially supersingular reduction is essential, as we now illustrate.

Let $K = \mathbb{Q}$ and let K_∞ be the unique $\mathbb{Z}_5^2$-extension of $\mathbb{Q}(i)$, so that

$$\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \mathbb{Z}_5 \times (\mathbb{Z}_5 \rtimes C_2).$$

Write K_n for the nth layer of K_∞/K, so $\mathrm{Gal}(K_n/\mathbb{Q}) \cong C_{5^n} \times D_{2\cdot 5^n}$.

Consider the following curves over $\mathbb{Q}$, which are connected by a 5-isogeny $\phi : E \to E'$:

$$E : y^2 + y = x^3 - x^2 - 8x - 7 \quad (75a1,\ \Delta_{E/\mathbb{Q}} = -3\cdot 5^4),$$
$$E' : y^2 + y = x^3 - x^2 + 42x + 443 \quad (75a2,\ \Delta_{E'/\mathbb{Q}} = -3^5\cdot 5^8).$$

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

They have non-split multiplicative reduction at $p = 3$, of Kodaira types I_1 and I_5, respectively, and additive potentially supersingular reduction at $p = 5$, of Kodaira types IV and IV*, respectively. Their periods are

$$\Omega_{E/\mathbb{Q}} = 1.4025\ldots = \Omega_{E'/\mathbb{Q}}, \quad \Omega^*_{E/\mathbb{R}} = 1.6646\ldots = 5\Omega^*_{E'/\mathbb{R}}.$$

Both curves have trivial torsion over $\mathbb{Q}(i)$ and therefore no 5-torsion over K_n, by Nakayama's lemma.

By Corollary 3.2,

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{5^\infty}(E/K_n)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{5^\infty}(E'/K_n)[\phi^t]|}\frac{|\text{Ш}^{\circ}_{E/K_n}[5^\infty]|}{|\text{Ш}^{\circ}_{E'/K_n}[5^\infty]|} = \left(\frac{\Omega_{E'/K}}{\Omega_{E/K}}\right)^{2\cdot 5^{2n}}\left(\frac{\Omega^*_{E'/\mathbb{R}}}{\Omega^*_{E/\mathbb{R}}}\right)^{5^{2n}}$$
$$\times \prod_{v|3}\frac{c_v(E'/K_n)}{c_v(E/K_n)}\prod_{v|5}\frac{c_v(E'/K_n)}{c_v(E/K_n)}\prod_{v|5}\left|\frac{\omega^{\min}_{E',5}/\omega^{\min}_{E',v}}{\omega^{\min}_{E,5}/\omega^{\min}_{E,v}}\right|_v.$$

The prime $p = 3$ is inert in $\mathbb{Q}(i)$ and in the 5-cyclotomic tower, and the prime above it in $\mathbb{Q}(i)$ is totally split in the 5-anticyclotomic tower of $\mathbb{Q}(i)$. So there are 5^n primes above 3 in K_n. The curves E and E' have split multiplicative reduction at each of them (of types I_1 and I_5), and so

$$\prod_{v|3}\frac{c_v(E'/K_n)}{c_v(E/K_n)} = 5^{5^n}.$$

The Tamagawa numbers at $v\,|\,5$ in K_n are coprime to 5 (potentially good reduction), but they do contribute to the quotient of ω terms. Specifically, there are two primes v_n^+ and v_n^- above 5 in K_n (one above $2+i$ and one above $2-i$ in $\mathbb{Q}(i)$), both with residue degree 5^n and ramification degree 5^n.

Remark 2.5 lets us the compute the ω term. For $v = v_n^{\pm}$,

$$\mathrm{ord}_v\left(\frac{\omega^{\min}_{E,v}}{\omega^{\min}_{E,5}}\right) = \frac{1}{12}\,\mathrm{ord}_v\left(\frac{\Delta_{E/\mathbb{Q}}}{\Delta_{E/K_n}}\right).$$

The valuation $\mathrm{ord}_v(\Delta_{E/K_n}) \in \{0, 1, \ldots, 11\}$ is uniquely determined by the congruence

$$\mathrm{ord}_v(\Delta_{E/K_n}) \equiv \mathrm{ord}_v(\Delta_{E/\mathbb{Q}}) \equiv \mathrm{ord}_v(5^4) \mod 12.$$

Therefore

$$\frac{1}{12}\,\mathrm{ord}_v\left(\frac{\Delta_{E/\mathbb{Q}}}{\Delta_{E/K_n}}\right) = \left\lfloor\frac{4\cdot 5^n}{12}\right\rfloor.$$

Similarly, the corresponding term for E' is $\lfloor(8\cdot 5^n)/12\rfloor$, and we find that

$$\left|\frac{\omega^{\min}_{E',5}/\omega^{\min}_{E',v}}{\omega^{\min}_{E,5}/\omega^{\min}_{E,v}}\right|_v = (5^{5^n})^{\lfloor(8\cdot 5^n)/12\rfloor - \lfloor(4\cdot 5^n)/12\rfloor} = (5^{5^n})^{(1/3)5^n-(1/3)(-1)^n} = 5^{(1/3)5^{2n}-(1/3)(-1)^n5^n}.$$

Putting everything together, we deduce that

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{5^\infty}(E/K_n)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{5^\infty}(E'/K_n)[\phi^t]|}\frac{|\text{Ш}^{\circ}_{E/K_n}[5^\infty]|}{|\text{Ш}^{\circ}_{E'/K_n}[5^\infty]|} = 1^{2\cdot 5^{2n}}\cdot 5^{-5^{2n}}\cdot 5^{5^n}\cdot[5^{(1/3)5^{2n}-(1/3)(-1)^n5^n}]^2$$
$$= 5^{-(1/3)5^{2n}+(1-(2/3)(-1)^n)\cdot 5^n}.$$

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

4. Minimal differentials

In this section we investigate the behaviour of the last term in Corollary 3.2 (the contribution from the exterior forms) in towers of local fields. We study its valuation, denoted by $\mathrm{Om}_\phi(\mathcal{F})$ below, and how it changes with $\mathcal{F}$.

Definition 4.1. Let $\mathcal{F}/\mathcal{K}$ be a finite extension of l-adic fields, and write $v_\mathcal{F}$ and $v_\mathcal{K}$ for their valuations. For an isogeny $\phi : A \to A'$ of abelian varieties over $\mathcal{K}$, define

$$\mathrm{Om}_\phi(\mathcal{F}) = v_\mathcal{F}\left(\frac{\omega^{\min}_{A'/\mathcal{F}}}{\omega^{\min}_{A'/\mathcal{K}}}\right) - v_\mathcal{F}\left(\frac{\omega^{\min}_{A/\mathcal{F}}}{\omega^{\min}_{A/\mathcal{K}}}\right),$$

so that

$$|k_\mathcal{F}|^{\mathrm{Om}_\phi(\mathcal{F})} = \left|\frac{\omega^{\min}_{A'/\mathcal{K}}/\omega^{\min}_{A'/\mathcal{F}}}{\omega^{\min}_{A/\mathcal{K}}/\omega^{\min}_{A/\mathcal{F}}}\right|_\mathcal{F},$$

where $k_\mathcal{F}$ is the residue field of $\mathcal{F}$ and $|\cdot|_\mathcal{F}$ the normalised absolute value.

Lemma 4.2. (i) *If $A, A'/\mathcal{K}$ are semistable, then $\mathrm{Om}_\phi(\mathcal{F}) = 0$ for every $\mathcal{F}/\mathcal{K}$.*

(ii) *If $\mathcal{F}'/\mathcal{F}/\mathcal{K}$ are finite and $\mathcal{F}'/\mathcal{F}$ is unramified, then $\mathrm{Om}_\phi(\mathcal{F}) = \mathrm{Om}_\phi(\mathcal{F}')$.*

Proof. (i) The minimal models of A and A' and the minimal exterior forms over $\mathcal{K}$ stay minimal over $\mathcal{F}$.

(ii) Ditto for $\mathcal{F}'/\mathcal{F}$. □

We now restrict our attention to elliptic curves. The term $v_\mathcal{F}(\omega^{\min}_{E/\mathcal{F}}/\omega^{\min}_{E/\mathcal{K}})$ measures the extent to which the minimal Weierstrass model of $E/\mathcal{K}$ fails to stay minimal over $\mathcal{F}$, and $\mathrm{Om}_\phi(\mathcal{F})$ is zero if the models of E and E' change by the same amount. The relation to minimal discriminants is as follows.

Notation 4.3. Let $\phi : E \to E'$ be an isogeny of elliptic curves over $\mathcal{K}$. Write

$$\delta = v_\mathcal{K}(\Delta_{E/\mathcal{K}}), \quad \delta' = v_\mathcal{K}(\Delta_{E'/\mathcal{K}}), \quad \delta_\mathcal{F} = v_\mathcal{F}(\Delta_{E/\mathcal{F}}), \quad \delta'_\mathcal{F} = v_\mathcal{F}(\Delta_{E'/\mathcal{F}})$$

for the valuations of the minimal discriminants.

Lemma 4.4. *If $\mathcal{F}/\mathcal{K}$ has ramification degree e, then*

$$\mathrm{Om}_\phi(\mathcal{F}) = \frac{e\delta' - \delta'_\mathcal{F}}{12} - \frac{e\delta - \delta_\mathcal{F}}{12} = \frac{e(\delta' - \delta)}{12} - \frac{\delta'_\mathcal{F} - \delta_\mathcal{F}}{12}.$$

Proof. Using [Sil86, Table III.1.2], we find that

$$v_\mathcal{F}\left(\frac{\omega^{\min}_{E/\mathcal{F}}}{\omega^{\min}_{E/\mathcal{K}}}\right) = \frac{1}{12} v_\mathcal{F}\left(\frac{\Delta_{E/\mathcal{K}}}{\Delta_{E/\mathcal{F}}}\right) = \frac{e\delta - \delta_\mathcal{F}}{12},$$

and similarly for E'. □

Theorem 4.5. *Let $\mathcal{F}/\mathcal{K}$ be a finite extension of l-adic fields of ramification degree e, and let $\phi : E \to E'$ be an isogeny of elliptic curves over $\mathcal{K}$. Then*

$$\mathrm{Om}_\phi(\mathcal{F}) = e\mu + \epsilon(\mathcal{F})$$

and

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

(i) $\mu = \epsilon(\mathcal{F}) = 0$ *if* $l \nmid \deg \phi$*, or* $E/\mathcal{K}$ *has good, potentially ordinary or potentially multiplicative reduction.*

Suppose that E *has additive potentially good reduction. Write* $\delta = v_{\mathcal{K}}(\Delta_{E/\mathcal{K}})$ *and* $\delta' = v_{\mathcal{K}}(\Delta_{E'/\mathcal{K}})$*. Write*[4] $\eth = 0, 2, 3, 4, 6, 8, 9$ *or* 10 *if* E *has Kodaira type* I_0, II, III, IV, $\mathrm{I}^*_{n\geqslant 0}$, IV^*, III^* *or* II^**, respectively, and similarly* $\eth'$ *for* E'*. Then:*

(ii) $\mu = (\delta' - \delta)/12$ *and* $\epsilon(\mathcal{F}) = \{e\delta/12\} - \{e\delta'/12\}$ *if* E *has tame reduction;*

(iii) $\mu = (\eth' - \eth)/12$ *and* $\epsilon(\mathcal{F}) = \{e\eth/12\} - \{e\eth'/12\}$ *if* $\mathcal{F}/\mathcal{K}$ *is tamely ramified;*

(iv) $\mu = (\delta' - \delta)/12$ *and* $|\epsilon(\mathcal{F})| \leqslant \frac{2}{3}$ *if* $l \neq 2$*; if, moreover,* $3 \mid e$*, then* $|\epsilon(\mathcal{F})| \leqslant \frac{1}{2}$*;*

(v) $\mu = (\delta' - \delta)/12$ *and* $|\epsilon(\mathcal{F})| < (re_{\mathcal{L}/\mathcal{K}} + 1)/2$ *if* $l = 2$*; here* r *is any real number satisfying* $r > f_{E/\mathcal{K}}/2 - 1$*, where* $f_{E/\mathcal{K}}$ *is the conductor exponent of* E*, and* $\mathcal{L}$ *is the subfield of* $\mathcal{F}$ *cut out by the upper ramification group* $I^r_{\mathcal{K}}$*.*

Proof. By Lemma 4.4,

$$\mathrm{Om}_{\phi}(\mathcal{F}) = \frac{e\delta' - \delta'_{\mathcal{F}}}{12} - \frac{e\delta - \delta_{\mathcal{F}}}{12} = \frac{e(\delta' - \delta)}{12} + \frac{\delta_{\mathcal{F}} - \delta'_{\mathcal{F}}}{12}. \qquad (\dagger)$$

The claims are trivial if ϕ is an endomorphism $E \to E$. Decomposing the isogeny if necessary, it is clear that in (i)–(iii) we may assume that $\deg \phi = p$ is prime.

(i) [DD15, Theorem 5.1] (or [DD15, Table 1]) describes the change in the discriminant under isogenies of prime degree. If E has potentially good reduction, and if either $l \neq p$ or E has good or potentially ordinary reduction, then $\delta = \delta'$ and $\delta_{\mathcal{F}} = \delta'_{\mathcal{F}}$. If E has potentially multiplicative reduction, then $\delta' - \delta = v_{\mathcal{K}}(j_E) - v_{\mathcal{K}}(j_{E'})$, and similarly $\delta'_{\mathcal{F}} - \delta_{\mathcal{F}} = e(v_{\mathcal{K}}(j_E) - v_{\mathcal{K}}(j_{E'}))$. In both cases the right-hand side of (†) is 0.

(ii) If $E/\mathcal{K}$ has tame reduction, the reduction stays tame over $\mathcal{F}$. Furthermore, we have that $0 \leqslant \delta, \delta', \delta_{\mathcal{F}}, \delta'_{\mathcal{F}} < 12$ by [DD15, Theorem 3.1]. Because the discriminant changes by 12th powers when the model is changed,

$$\delta_{\mathcal{F}} = 12\left\{\frac{e\delta}{12}\right\}, \quad \delta'_{\mathcal{F}} = 12\left\{\frac{e\delta'}{12}\right\},$$

and (†) implies the asserted formula.

(iii) By [DD13, Theorem 3],

$$\delta_{\mathcal{F}} = e\delta - 12\left\lfloor\frac{e\eth}{12}\right\rfloor, \quad \delta'_{\mathcal{F}} = e\delta' - 12\left\lfloor\frac{e\eth'}{12}\right\rfloor,$$

and the claim follows from (†).

(iv) Write m and m' for the numbers of components of the Néron minimal models of $E/\mathcal{F}$ and $E'/\mathcal{F}$, respectively. As $l \neq 2$, by [Sil94, § IV.9, Table 4.1] the curves E and E' do not have Kodaira type $\mathrm{I}^*_{n>0}$, and $1 \leqslant m, m' \leqslant 9$. Since E and E' have the same conductor exponent (over $\mathcal{F}$), by Ogg's formula [Sil94, IV.11.1] we have that

$$|\delta_{\mathcal{F}} - \delta'_{\mathcal{F}}| = |m - m'| \leqslant 8.$$

Therefore, by (†),

$$\mathrm{Om}_{\phi}(\mathcal{F}) = \frac{e(\delta' - \delta)}{12} + \epsilon(\mathcal{F}), \quad |\epsilon(\mathcal{F})| \leqslant \frac{2}{3}.$$

If, moreover, $3 \mid e$, then $3 \mid \delta_{\mathcal{F}}, \delta'_{\mathcal{F}}$. In this case $|\delta_{\mathcal{F}} - \delta'_{\mathcal{F}}| \leqslant 6$ and $|\epsilon(\mathcal{F})| \leqslant \frac{1}{2}$.

[4] We use $\eth$ (Icelandic letter 'eth') as it is a relative of the letter δ.

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

(v) By Ogg's formula and [Pap93, Theorem 2], we have $f_{E/\mathcal{F}} \leqslant \delta_{\mathcal{F}} \leqslant 4f_{E/\mathcal{F}}$. As E and E' have the same conductor, the same bounds hold for $\delta'_{\mathcal{F}}$, and so $|\delta_{\mathcal{F}} - \delta'_{\mathcal{F}}| \leqslant 3f_{E/\mathcal{F}}$. By Theorem A.4 in the Appendix,

$$f_{E/\mathcal{F}} = f_{E/\mathcal{L}} \leqslant e_{\mathcal{L}/\mathcal{K}}(f_{E/\mathcal{K}} - 2) + 2.$$

Therefore

$$\frac{|\delta_{\mathcal{F}} - \delta'_{\mathcal{F}}|}{12} \leqslant \frac{e_{\mathcal{L}/\mathcal{K}}}{4}(f_{E/\mathcal{K}} - 2) + \frac{1}{2} < \frac{e_{\mathcal{L}/\mathcal{K}}}{4} \cdot 2r + \frac{1}{2} = \frac{re_{\mathcal{L}/\mathcal{K}} + 1}{2}.$$

The claim follows from (†), with $\epsilon(\mathcal{F}) = (\delta_{\mathcal{F}} - \delta'_{\mathcal{F}})/12$. □

Remark 4.6. Note that in Theorem 4.5(iii), the formula $\mu = (\eth' - \eth)/12$ may *not* be replaced by $(\delta' - \delta)/12$. For example, the 2-isogenous curves 64a1 and 64a4 over $\mathbb{Q}_2$ have type $\mathrm{I}_2^*, \delta = 12, \eth = 6$ and type II, $\delta' = 6, \eth' = 2$, respectively, and $\delta' - \delta \neq \eth' - \eth$. If $E/\mathcal{K}$ has tame reduction, e.g. when $\mathcal{K}$ has residue characteristic at least 5, then $\delta = \eth$ and the two formulae are the same.

COROLLARY 4.7. *Let $\mathcal{K}_n = \mathbb{Q}_l(p^n)$ be the completion of the nth layer of the p-cyclotomic tower at a prime above l, and let $\phi : E \to E'$ be an isogeny of elliptic curves over $\mathbb{Q}_l$. Then*

$$\mathrm{Om}_\phi(\mathcal{K}_n) = p^n\mu + \epsilon(n),$$

and $\mu = \epsilon(n) = 0$ unless $l = p \mid \deg\phi$ and E has additive potentially supersingular reduction. In this exceptional case, writing $\delta = \mathrm{ord}_l\,\Delta_{E/\mathbb{Q}_l}$ and $\delta' = \mathrm{ord}_l\,\Delta_{E'/\mathbb{Q}_l}$, we have

$$\mu = \frac{\delta' - \delta}{12}, \quad |\epsilon(n)| \leqslant \begin{cases} \dfrac{2}{3} & \text{if } l \geqslant 5, \\ \dfrac{1}{2} & \text{if } l = 3, \\ 6\dfrac{1}{2} & \text{if } l = 2. \end{cases}$$

If, moreover, E has tame reduction, then $\epsilon(n) = \{p^n\delta/12\} - \{p^n\delta'/12\}$.

Proof. If $l \neq p$, then $\mathrm{Om}_\phi = 0$ by Lemma 4.2(ii). If $l \nmid \deg\phi$, or if $E/\mathcal{K}$ has good, potentially ordinary or potentially multiplicative reduction, then $\mathrm{Om}_\phi = 0$ as well, by Theorem 4.5(i). Assume henceforth that $l = p \mid \deg\phi$ and E has additive potentially supersingular reduction.

The last claim for $\epsilon(n)$ is contained in Theorem 4.5(ii), and the assertion for $l \geqslant 3$ was proved in Theorem 4.5(iv).

Finally, suppose $l = 2$. By Theorem 4.5(v), the asserted equality holds with $|\epsilon(n)| < (re + 1)/2$, where $r > f_{E/\mathbb{Q}_2}/2 - 1$ and e is the ramification degree of the field cut out by $I^r_{\mathbb{Q}_2}$. By [LRS93] we have $f_{E/\mathbb{Q}_2} \leqslant 2 + 6v_{\mathbb{Q}_2}(2) = 8$. So we can take $3 < r < 4$, $\mathcal{L} = \mathbb{Q}_2(2^2)$ and $e = 4$ (or $\mathcal{L} = \mathbb{Q}_2(2)$ and $e = 2$ if $n = 1$). Then $|\epsilon(n)| < (re + 1)/2 \leqslant (4r + 1)/2$, which gives the bound of 6.5 as $r \to 3$. □

Remark 4.8. If $l = p > 3$, then every curve over $\mathcal{K}$ with potentially good reduction is tame, so $\epsilon(n)$ in Corollary 4.7 is explicit. If $l \neq p$, it is zero, and for $l = p = 3$ it can be made explicit as well by using Ogg's formula as follows.

Suppose that $E/\mathcal{K}_n$ has wild reduction for all n. The conductor exponent of $E/\mathcal{K}_n$ stabilises by Corollary A.6 in the Appendix, and the number of components m on the Néron minimal model satisfies $1 \leqslant m \leqslant 9$ (cf. the proof of Theorem 4.5(iv)). Therefore the congruence $\delta_{\mathcal{K}_n} \equiv e_{\mathcal{K}_n/\mathbb{Q}_l}\delta$ mod 12 determines both m and $\delta_{\mathcal{K}_n}$ uniquely. The same is true for E', and we get an explicit formula for $\epsilon(n) = (\delta_{\mathcal{K}_n} - \delta'_{\mathcal{K}_n})/12$ for large n.

Let us also observe that $\epsilon(n) \in \{-\frac{1}{2}, 0, \frac{1}{2}\}$ for large n in this case. Indeed, the ramification degree $e_{\mathcal{K}_n/\mathbb{Q}_l}$ is divisible by 3, and so $\delta_{\mathcal{K}_n} - \delta'_{\mathcal{K}_n}$ is also divisible by 3. By Lemma 2.4 and Theorem 4.5(iv),

$$\left| \frac{\delta_{\mathcal{K}_n} - \delta'_{\mathcal{K}_n}}{12} \right| = |\epsilon(n)| \leqslant \frac{1}{2},$$

and so $|\delta_{\mathcal{K}_n} - \delta'_{\mathcal{K}_n}| \leqslant 6$. Moreover, $\delta_{\mathcal{K}_n} - 3\delta'_{\mathcal{K}_n} \equiv 0 \bmod 4$ (see [DD15, Theorem 1.1]), so $\delta_{\mathcal{K}_n}$ and $\delta'_{\mathcal{K}_n}$ have the same parity, whence $\delta_{\mathcal{K}_n} - \delta'_{\mathcal{K}_n} \in \{-6, 0, 6\}$.

5. Tamagawa numbers

We now turn to the behaviour of the Tamagawa number quotient from Corollary 3.2 in towers of l-adic fields.

Theorem 5.1. *Let $\mathcal{K} = \mathcal{K}_0 \subset \mathcal{K}_1 \subset \mathcal{K}_2 \subset \cdots$ be a tower of l-adic fields, and let $\phi : E \to E'$ be an isogeny of elliptic curves over $\mathcal{K}$. Then the sequence*

$$\frac{c_{E'/\mathcal{K}_0}}{c_{E/\mathcal{K}_0}}, \quad \frac{c_{E'/\mathcal{K}_1}}{c_{E/\mathcal{K}_1}}, \quad \frac{c_{E'/\mathcal{K}_2}}{c_{E/\mathcal{K}_2}}, \ldots$$

stabilises unless $l \mid \deg\phi$, $e_{\mathcal{K}_n/\mathcal{K}} \to \infty$ and $E/\mathcal{K}$ has wild potentially supersingular reduction (in particular $l = 2, 3$). In this exceptional case, and in all other cases where E has potentially good reduction, all terms in the sequence lie in $\{1, 2, 3, 4, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}\}$.

Proof. First, if $e_{\mathcal{K}_n/\mathcal{K}} \not\to \infty$, then the extensions $\mathcal{K}_{n+1}/\mathcal{K}_n$ are eventually unramified, so the Tamagawa numbers of E and E' stabilise.

Next, suppose that either $l \nmid \deg\phi$ or E is not wild potentially supersingular. If $E = E'$, there is nothing to prove. Otherwise, by decomposing ϕ into endomorphisms and isogenies of prime degree if necessary, we may assume that $\deg\phi = p$ is prime. Now apply the classification for the quotient c/c' from [DD15, Table 1]. All the conditions in the table that determine c/c' (i.e. that E is good, ordinary, additive, split multiplicative, has non-trivial 3-torsion, $v(j_E) = pv(j_{E'})$, etc.) stabilise in the tower $\mathcal{K}_n$, and hence so does the quotient.

Now suppose that E and E' have potentially good reduction. In particular, the reduction is good or additive over all $\mathcal{K}_n$, and so $1 \leqslant c_{E/\mathcal{K}_n}, c_{E'/\mathcal{K}_n} \leqslant 4$ (see [Sil94, § IV.9, Table 4.1]). To prove the claim, it suffices to check that if one of them, say $c_{E/\mathcal{K}_n}$, is 3, then the other cannot be 2 or 4. Indeed, $c_{E/\mathcal{K}_n} = 3$ implies that E has Kodaira type IV or IV* and $c_{E'/\mathcal{K}_n} \in \{2, 4\}$ implies that E' has type III, III*, I$_0^*$ or I$_n^*$ (see [Sil94, § IV.9, Table 4.1]). Such curves cannot be isogenous, because: (a) for $l = 2$ the former types are tame and the latter are wild [KT82, Proposition 8.20]; (b) for $l = 3$ the former types are wild and the latter are tame [Kra90, Theorem 1]; and (c) for $l > 3$ the curve E' also has type IV or IV*, e.g. from [DD15, Table 1] or by considering the valuations of minimal discriminants and the smallest fields where the curves acquire good reduction. □

Remark 5.2. If $\deg\phi$ is a prime $p \geqslant 5$, then the quotient $c(E'/\mathcal{K}_n)/c(E/\mathcal{K}_n)$ is particularly simple. It stabilises to:

- p if $E/\mathcal{K}_n$ has split multiplicative reduction for some n, and $v_{\mathcal{K}}(j_{E'})/v_{\mathcal{K}}(j_E) = p$;
- $1/p$ if $E/\mathcal{K}_n$ has split multiplicative reduction for some n, and $v_{\mathcal{K}}(j_{E'})/v_{\mathcal{K}}(j_E) = 1/p$;
- 1 in all other cases.

Corollary 5.3. *If $\phi : E \to E'$ is an isogeny of elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}(l^n)$ is the nth layer in the l-cyclotomic tower, then the sequence*

$$\prod_v \frac{c_v(E'/\mathbb{Q}(l^n))}{c_v(E/\mathbb{Q}(l^n))}$$

stabilises, unless $l \mid \deg\phi$ and E has wild potentially supersingular reduction at l (in particular, $l = 2, 3$). In this exceptional case, for all sufficiently large n, the terms are of the form $C \cdot \alpha_n$ for some constant C and some $\alpha_n \in \{1, 2, 3, 4, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}\}$.

Remark 5.4. For elliptic curves with wild potentially supersingular reduction, the quotient of Tamagawa numbers might *not* stabilise.

As an example, take the 3-isogeny $E = 243a1 \to 243a2 = E'$ over $\mathbb{Q}(3^n)$, and consider the Tamagawa numbers at primes above 3. As in Remark 4.8, one may compute the minimal discriminants and the number of components of the Néron minimal model (and thus the Kodaira types). We find that the Kodaira types of E, E' alternate between $\mathrm{IV}^*, \mathrm{II}$ and $\mathrm{II}^*, \mathrm{IV}$. The Tamagawa numbers for types II and II^* are always 1 (see [Sil94, § IV.9, Table 4.1]), and they turn out to be 3 for the IV and IV^* cases, so that the Tamagawa quotient alternates between 3 and $\frac{1}{3}$. (To see that the Tamagawa numbers are 3, we use the fact that over a local field $\mathcal{K}/\mathbb{Q}_3$, the parity of $\mathrm{ord}_3\,(c(E'/\mathcal{K})/c(E/\mathcal{K}))$ can be recovered from $\mathrm{Om}_\phi(\mathcal{K})$, the local root number $w(E/\mathcal{K})$, and the Artin symbol $(-1, \mathcal{K}(\ker\phi^t)/\mathcal{K})$; see [DD11, Theorem 5.7]. In our case, $\mathrm{Om}_\phi(\mathcal{K})$ is computed as in Remark 4.8, the local root number is $+1$ over $\mathbb{Q}_3$ and is unchanged in odd-degree Galois extensions, and the points in $\ker\phi^t$ are defined over $\mathbb{Q}$, so that the Artin symbol is trivial.)

Finally, we record the fact that Theorem 5.1 also holds for semistable abelian varieties.

Theorem 5.5. *Let $\mathcal{K} \subset \mathcal{K}_1 \subset \mathcal{K}_2 \subset \cdots$ be a tower of l-adic fields, and let $\phi : A \to A'$ be an isogeny of semistable abelian varieties over $\mathcal{K}$. Then the quotient of Tamagawa numbers $c(A'/\mathcal{K}_n)/c(A/\mathcal{K}_n)$ stabilises as $n \to \infty$.*

Proof. By [BD14, Corollary 3.2.8], for sufficiently large n,

$$c(A/\mathcal{K}_n) = C \cdot e^r_{\mathcal{K}_n/\mathcal{K}} \quad \text{and} \quad c(A'/\mathcal{K}_n) = C' \cdot e^r_{\mathcal{K}_n/\mathcal{K}}$$

for some constants C and C'. Here e is the ramification degree, and r denotes the rank of the split toric part of $A/\mathcal{K}_n$ (and of $A'/\mathcal{K}_n$) for large enough n. The claim follows. □

6. Torsion

To deduce the exact growth of Ш from the isogeny invariance of the Birch–Swinnerton-Dyer conjecture, we need to control torsion in the Mordell–Weil group in towers of number fields. This is the purpose of this section.

Proposition 6.1. *Let $K \subset K_1 \subset K_2 \subset \cdots$ be a tower of number fields, and let $\phi : A \to A'$ be an isogeny of abelian varieties over K of degree $p^k m$, with $p \nmid m$. Then for every $n \geqslant 1$,*

$$\frac{|A(K_n)[p^\infty]|}{|A'(K_n)[p^\infty]|} = p^{a_n} \quad \textit{with} \;\; k(1 - 2\dim A) \leqslant a_n \leqslant k.$$

If A has finite p-power torsion over $\bigcup_n K_n$, then the quotient stabilises.

Proof. Because $\phi : A(K_n)[p^\infty] \to A'(K_n)[p^\infty]$ has kernel of size at most p^k, the left-hand side quotient is at most p^k. The same argument applied to the conjugate isogeny $\phi' : A' \to A$ (with $\phi \circ \phi'$ the multiplication-by-p^k map) gives the first claim. The second claim is clear, as both $A(K_n)[p^\infty]$ and $A'(K_n)[p^\infty]$ stabilise. $\square$

Corollary 6.2. *Let K be a number field, $K_\infty = \bigcup_n K_n$ its cyclotomic $\mathbb{Z}_l$-extension, and A, A'/K isogenous abelian varieties. Then for every prime p the sequence $|A(K_n)[p^\infty]|/|A'(K_n)[p^\infty]|$ stabilises as $n \to \infty$.*

Proof. By the Imai–Serre theorem (see, e.g., [Rib81]), A has finite torsion over K_∞. $\square$

Remark 6.3. If $A = E$ is an elliptic curve over $K = \mathbb{Q}$ and the $K_n/\mathbb{Q}$ are Galois, the assumption that E has finite p-power torsion over $K_\infty = \bigcup_n K_n$ simply means that K_∞ does not contain the full p-division tower $\mathbb{Q}(E[p^\infty])$. Indeed, if E/K_∞ has infinite p-power torsion and $K_\infty/\mathbb{Q}$ is Galois but does not contain $\mathbb{Q}(E[p^\infty])$, then $E[p^n]$ has a Galois stable cyclic subgroup of order p^n and hence a cyclic p^n-isogeny for every $n \geqslant 1$. Since E cannot have CM over $\mathbb{Q}$, this is impossible by Shafarevich's theorem on the finiteness of isogeny classes.

7. Divisible Selmer

The ultimate global invariant that we need to control is the divisible part of the p^∞-Selmer group. Its $\mathbb{Z}_p$-corank $\mathrm{rk}_p\, A/K$ is conjecturally the Mordell–Weil rank, which is hard to bound in general towers of number fields K_n/K. As a result, we only give elementary bounds on $|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K_n)[\phi]|$ in terms of $\mathrm{rk}_p\, A/K_n$ and prove some stabilisation results that we will need in § 8.

Lemma 7.1. *Let $\phi : A \to A'$ be an isogeny of abelian varieties over a number field K, and let p be a prime number. Then*

$$|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K)[\phi]| \leqslant p^{\mathrm{rk}_p A/K \cdot \mathrm{ord}_p \deg \phi}.$$

Proof. Let $d = \deg \phi$, and let ϕ' be the conjugate isogeny, so that $\phi' \circ \phi$ is multiplication by d. Then it is clear that

$$\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K)[\phi] \subset \mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K)[d].$$

The right-hand side has size $p^{\mathrm{rk}_p A/K \cdot \mathrm{ord}_p d}$, since $\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K)$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rk}_p A/K}$. $\square$

Corollary 7.2. *Let $K \subset K_1 \subset K_2 \subset \cdots$ be a tower of number fields, $\phi : A \to A'$ an isogeny of abelian varieties over K, and p a prime number. Then*

$$\mathrm{ord}_p \frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A'^t/K)[\phi^t]|} = O(\mathrm{rk}_p\, A/K_n).$$

Proof. Apply Lemma 7.1 to ϕ and ϕ^t. $\square$

Lemma 7.3. *Let F/K be a Galois extension of number fields and A/K an abelian variety. Then*

$$|\ker(\mathrm{Res} : \mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K) \to \mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/F))| \leqslant |A(F)[p^\infty]|^{\mathrm{rk}_p A/K}.$$

Proof. First observe that for every $n \geqslant 1$,

$$\ker(\mathrm{Res} : \mathrm{Sel}_{p^n}(A/K) \to \mathrm{Sel}_{p^n}(A/F))$$

is killed by $M = |A(F)[p^\infty]|$. Indeed, $\mathrm{Sel}_{p^n}(A/K) \subset H^1(K, A[p^n])$, and the kernel of

$$\mathrm{Res} : H^1(K, A[p^n]) \to H^1(F, A[p^n])$$

is $H^1(\mathrm{Gal}(F/K), A(F)[p^n])$ by the inflation–restriction sequence, and so is clearly killed by M. Because Sel_{p^∞} is the injective limit of the Sel_{p^n}, the asserted kernel on Sel_{p^∞} and on $\mathrm{Sel}_{p^\infty}^{\mathrm{div}}$ is also killed by M. As $\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rk}_p A/K}$, the result follows. □

THEOREM 7.4. *Let K be a number field, A/K an abelian variety, p a prime number and $K \subset K_1 \subset K_2 \subset \cdots$ a tower of Galois extensions of K. Suppose that both $A(K_n)[p^\infty]$ and $\mathrm{rk}_p A/K_n$ are bounded as $n \to \infty$.*

(i) *There exists n_0 such that the restriction maps*

$$J_{n,n'} : \mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K_n) \longrightarrow \mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K_{n'})$$

are isomorphisms for all $n_0 \leqslant n \leqslant n'$.

(ii) *If $\phi : A \to A'$ is an isogeny, then $|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K_n)[\phi]|$ is eventually constant, equal to p^λ for some $0 \leqslant \lambda \leqslant \mathrm{ord}_p \deg \phi \cdot \lim_{n\to\infty} \mathrm{rk}_p A/K_n$.*

Proof. (i) Because $\mathrm{rk}_p A/K_n \leqslant \mathrm{rk}_p A/K_{n'}$ for $n \leqslant n'$, the p^∞-Selmer rank eventually stabilises. Replacing K by some K_m, we may thus assume that $\mathrm{rk}_p A/K_n$ is independent of n. The maps $J_{n,n'}$ have finite kernels by Lemma 7.3, so they must then be surjective.

By assumption, A has finite p-power torsion over $\bigcup K_n$, say of order M. The (increasing) sequence $|\ker J_{0,n}|$ is bounded by Lemma 7.3, so it stabilises, say at n_0. Now suppose $n_0 \leqslant n \leqslant n'$. The map $J_{n,n'}$ cannot have non-trivial kernel because $J_{0,n'} = J_{n,n'} \circ J_{0,n}$, the kernels of $J_{0,n}$ and $J_{0,n'}$ are of the same size, and $J_{0,n}$ is surjective. Thus the $J_{n,n'}$ are both surjective and injective, as required.

(ii) Take n_0 as above, so that $\mathrm{rk}_p A/K_n$ is constant and the $J_{n_0,n}$ are isomorphisms for $n \geqslant n_0$. Then, by Lemma 7.1, $|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K_{n_0})[\phi]| = p^\lambda$ for some $0 \leqslant \lambda \leqslant \mathrm{ord}_p \deg \phi \cdot \mathrm{rk}_p A/K_{n_0}$. Now the maps $J_{n_0,n}$ are isomorphisms and commute with ϕ, and the result follows. □

COROLLARY 7.5. *Let $K_\infty = \bigcup_n K_n$ be the l-cyclotomic tower of a number field K, and let $\phi : A \to A'$ be an isogeny of abelian varieties over K. If $\mathrm{rk}_p A/K_n$ is bounded as $n \to \infty$, then $|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(A/K_n)[\phi]|$ is eventually constant.*

Proof. For cyclotomic towers, torsion in $A(K_n)$ is bounded by the Imai–Serre theorem (see, e.g., [Rib81]). □

COROLLARY 7.6. *Let $\mathbb{Q}_\infty = \bigcup_n \mathbb{Q}(l^n)$ be the l-cyclotomic tower of $\mathbb{Q}$, and let $\phi : E \to E'$ be an isogeny of elliptic curves over $\mathbb{Q}$. Then $|\mathrm{Sel}_{p^\infty}^{\mathrm{div}}(E/\mathbb{Q}(l^n))[\phi]|$ is eventually constant.*

Proof. By Kato's theorem [Kat04], the p^∞-Selmer rank of E is bounded in the cyclotomic tower. □

8. Selmer growth in towers

In this section we prove Theorems 1.1–1.3. The proofs rely on the invariance of the Birch–Swinnerton-Dyer conjecture under isogeny (as in § 3) and the explicit computations of the periods Ω_A and $\Omega_{A'}$, the exterior form contributions Om_ϕ, and the Tamagawa numbers and torsion from §§ 2, 4, 5 and 6. In fact, Theorem 8.2 and Proposition 8.5 give an explicit description of the Selmer quotient in almost completely general towers of number fields. To obtain the statements for Ш, we also bound the contributions from the divisible part of Selmer using the results of § 7.

Notation 8.1. Let F/K be a Galois extension of number fields, and let $\phi : A \to A'$ be an isogeny of abelian varieties over K. For a place v of K and a place $w \,|\, v$ of F write

$$\gamma_v = \begin{cases} \dfrac{\Omega^*_{A'/K_v}}{\Omega^*_{A/K_v}} & \text{if } K_v \cong \mathbb{R}, F_w \cong \mathbb{C}, \\ 1 & \text{in all other Archimedean cases,} \\ \dfrac{c_w(A'/F)}{c_w(A/F)} |k_w|^{\mathrm{Om}_\phi(F_w)} & \text{if } v \nmid \infty, \end{cases}$$

where k_w is the residue field at w and Om_ϕ is as in Definition 4.1. Note that $\gamma_v = 1$ for primes of v of good reduction; see Lemma 4.2.

If $K \subset K_1 \subset K_2 \subset \cdots$ is a tower of Galois extensions of K, we write $e_{v,n}, f_{v,n}$ and $n_{v,n}$ for the ramification degree of v, the residue degree of v and the number of places above v in K_n/K, respectively. In this setting, we also write $\gamma_{v,n}$ for the γ_v for $F = K_n$.

Theorem 8.2. *Let F/K be a Galois extension of number fields, and let $\phi : A \to A'$ be an isogeny of abelian varieties over K. If the degree of ϕ is a power of p, then*

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/F)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A'^t/F)[\phi^t]|} \frac{|\text{Ш}^\circ_{A/F}[p^\infty]|}{|\text{Ш}^\circ_{A'/F}[p^\infty]|} = \frac{|A(F)[p^\infty]|\,|A^t(F)[p^\infty]|}{|A'(F)[p^\infty]|\,|A'^t(F)[p^\infty]|} \left(\frac{\Omega_{A'/K}}{\Omega_{A/K}}\right)^{[F:K]} \prod_v \gamma_v^{n_v},$$

where n_v is the number of places of F above v. If ϕ has arbitrary degree, then the left-hand side and right-hand side have the same p-part.

Proof. This is a rephrasing of Corollary 3.2. □

Theorem 8.3. *Let $\mathbb{Q}_\infty = \bigcup_n \mathbb{Q}(l^n)$ be the l-cyclotomic tower, p a prime, and $\phi : E \to E'$ an isogeny of elliptic curves over $\mathbb{Q}$. Then for all large enough n,*

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(E/\mathbb{Q}(l^n))[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(E'/\mathbb{Q}(l^n))[\phi^t]|} \frac{|\text{Ш}^\circ_{E/\mathbb{Q}(l^n)}[p^\infty]|}{|\text{Ш}^\circ_{E'/\mathbb{Q}(l^n)}[p^\infty]|} = p^{\mu l^n + \kappa + \epsilon(n)},$$

with $\mu \in \frac{1}{12}\mathbb{Z}$ given by

$$\mu = \mathrm{ord}_p \frac{\Omega_{E'}}{\Omega_E} + \begin{cases} 0 & \text{if } l \neq p \text{ or } \mathrm{ord}_p(j_E) < 0, \\ \dfrac{1}{12}\mathrm{ord}_p\left(\dfrac{\Delta_{E'}}{\Delta_E}\right) & \text{if } l = p \text{ and } \mathrm{ord}_p(j_E) \geqslant 0, \end{cases}$$

some $\kappa \in \mathbb{Z}$, and $|\epsilon(n)| \leqslant \frac{2}{3}$ for $p > 3$, $|\epsilon(n)| \leqslant \frac{3}{2}$ for $p = 3$ and $|\epsilon(n)| \leqslant 8\frac{1}{2}$ for $p = 2$. If $l \neq p$ or $l \nmid \deg \phi$, then $\epsilon(n) = 0$.

Proof. To find the Selmer quotient, we apply Theorem 8.2. The torsion contribution is eventually constant by Corollary 6.2. Now compute the $\gamma_{v,n}$ (see Notation 8.1) for $K_n = \mathbb{Q}(l^n)$ and all primes v of $\mathbb{Q}$. By Corollary 5.3, the product of Tamagawa quotients stabilises unless $l \leqslant 3$, $l \mid \deg\phi$ and E has wild potentially supersingular reduction at l. In that case, the term is of the form $l^{\xi(n)}$ with $|\xi(n)| \leqslant 1$ when $l = 3$ and $|\xi(n)| \leqslant 2$ when $l = 2$. By Corollary 4.7, the Om_ϕ term is 1 unless $l = p$ and E has additive potentially supersingular reduction at l, in which case it is

$$p^{(l^n/12)\mathrm{ord}_p(\Delta_{E'}/\Delta_E)+\eta(n)},$$

with $|\eta(n)|$ bounded by $\frac{2}{3}$, $\frac{1}{2}$ and $6\frac{1}{2}$ for $p > 3$, $p = 3$ and $p = 2$, respectively. The claim follows, with the asserted bounds for $\epsilon(n) = \xi(n) + \eta(n)$. □

Corollary 8.4. *Theorem 1.1 holds.*

Proof. Combine Theorem 8.3 and Corollary 7.6. □

Proposition 8.5. *Let $K \subset K_1 \subset K_2 \subset \cdots$ be a tower of Galois extensions of K, and let $\phi : A \to A'$ be an isogeny of abelian varieties over K. For a prime v of K and a rational prime p,*

(i) *if $v \nmid p$, or A is semistable at v, or A is an elliptic curve which does not have additive potentially supersingular reduction at v, then $\mathrm{ord}_p\,\gamma_{v,n}$ is constant for sufficiently large n.*

Suppose that $v \mid p$ and that $A = E$ and $A' = E'$ are elliptic curves with potentially good reduction at v. Write $\delta = \delta_{E/K_v}, \delta' = \delta_{E'/K_v}, \eth = \eth_{E/K_v}$ and $\eth' = \eth_{E'/K_v}$ as in Theorem 4.5. Then, for all sufficiently large n,

$$\mathrm{ord}_p\,\gamma_{v,n} = \mu_v e_{v,n} f_{v,n} + \epsilon_{v,n} f_{v,n} f_{K_v/\mathbb{Q}_p} + z_n,$$

with:

(ii) *$\mu_v = f_{K_v/\mathbb{Q}_p}(\delta' - \delta)/12$, $\epsilon_{v,n} = \{e_{v,n}\delta/12\} - \{e_{v,n}\delta'/12\}$, and z_n constant if E has tame reduction at v;*

(iii) *$\mu_v = f_{K_v/\mathbb{Q}_p}(\eth' - \eth)/12$, $\epsilon_{v,n} = \{e_{v,n}\eth/12\} - \{e_{v,n}\eth'/12\}$, and $|z_n| \leqslant 2$ if all K_n/K are tamely ramified at v;*

(iv) *$\mu_v = f_{K_v/\mathbb{Q}_p}(\delta' - \delta)/12$, $|\epsilon_{v,n}| \leqslant \frac{2}{3}$, and $|z_n| \leqslant 1$ if $p = 3$;*

(v) *$\mu_v = f_{K_v/\mathbb{Q}_p}(\delta' - \delta)/12$, $\epsilon_{v,n} = O(1)$, and $|z_n| \leqslant 2$ if $p = 2$ and all upper ramification subgroups of the inertia group $I_{\bigcup K_n/K}$ at v have finite index.*

Proof. Combine Lemma 4.2(i) with Theorems 4.5 and 5.1. □

Remark 8.6. For sufficiently large n, the constants $\mathrm{ord}_p\,\gamma_{v,n}$ in (i) and z_n in (ii) are just $\mathrm{ord}_p\,(c_w(A'/K_n)/c_w(A/K_n))$, where w is a prime of K_n above v. If K_∞/K_n is unramified at primes above v for n sufficiently large, then $z_n = \mathrm{ord}_p\,(c_w(A'/K_n)/c_w(A/K_n))$ and the $\epsilon_{v,n}$ are constants in (iii)–(v) as well, by Lemma 4.2(ii) and Theorem 5.1.

Theorem 8.7. *Let K be a number field, p a prime, and $K_\infty = \bigcup_n K_n$ a $\mathbb{Z}_l$-extension of K with $[K_n : K] = l^n$. Let $\phi : E \to E'$ be an isogeny of elliptic curves over K. Then*

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(E/K_n)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(E'/K_n)[\phi^t]|}\frac{|Ш^{\circ}_{E/K_n}[p^\infty]|}{|Ш^{\circ}_{E'/K_n}[p^\infty]|} = p^{\mu l^n + O(1)}, \quad \mu = \mathrm{ord}_p\left(\frac{\Omega_{E'/K}}{\Omega_{E/K}}\right) + \sum_v \mu_v,$$

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

where the sum is taken over the primes v of bad reduction for E/K and

$$\mu_v = \begin{cases} \operatorname{ord}_p \dfrac{c_v(E'/K)}{c_v(E/K)} & \text{if } v \text{ is totally split in } K_\infty/K,\\ \dfrac{f_{K_v/\mathbb{Q}_p}}{12}\operatorname{ord}_v\left(\dfrac{\Delta_{E'/K}}{\Delta_{E/K}}\right) & \text{if } l=p,\ v\,|\,p \text{ is ramified in } K_\infty/K \text{ and } \operatorname{ord}_v j_E \geqslant 0,\\ 0 & \text{otherwise.}\end{cases}$$

Proof. We apply Theorem 8.2. The torsion contribution is $O(1)$ by Proposition 6.1. All Archimedean places are totally split in K_∞/K, since $\mathbb{Z}_l$ has no elements of order 2, so $\gamma_{v,n}=1$ for $v\,|\,\infty$. It remains to show that $\operatorname{ord}_p(\gamma_{v,n}^{n_{v,n}}) = \mu_v l^n + O(1)$ for primes v of K of bad reduction for E and E'. Because the inertia and the decomposition subgroups at v are closed subgroups of $\mathbb{Z}_l$, the possible local behaviours of K_∞/K at v are:

(1) K_∞/K is totally split at v, so $n_{v,n}=l^n$, $e_{v,n}=1$ and $f_{v,n}=1$;

(2) K_∞/K is not totally split but unramified at v, so $n_{v,n}=c$, $e_{v,n}=1$ and $f_{v,n}=l^n/c$ for some constant c and all large enough n;

(3) K_∞/K is ramified at v, so $n_{v,n}=c_1$, $e_{v,n}=l^n/c_1c_2$ and $f_{v,n}=c_2$ for some constants c_1 and c_2 and all large enough n; here necessarily $v\,|\,l$.

In the first case, $\mathrm{Om}_\phi(K_{n,w})=0$ for $w\,|\,v$ since $K_{n,w}=K_v$, and hence $\operatorname{ord}_p(\gamma_{v,n}^{n_{v,n}}) = \mu_v l^n$. In the second case, Om_ϕ is still 0 by Lemma 4.2(ii), so $\gamma_{v,n}^{n_{v,n}}$ is a finite product of bounded quotients of Tamagawa numbers, which is $O(1)$.

Assume we are in the third case.

If $v\nmid p$ or E does not have additive potentially good reduction at v, then $\operatorname{ord}_p \gamma_{v,n}$ is eventually constant by Proposition 8.5(i), and hence so is $\operatorname{ord}_p(\gamma_{v,n}^{n_{v,n}})$; in particular, it is again $O(1)$. Also $\mu_v=0$: either $v\nmid p$, or E and E' have good reduction at v and $\operatorname{ord}_v \Delta_{E/K} = \operatorname{ord}_v \Delta_{E'/K}=0$, or E and E' have potentially multiplicative reduction (i.e. $\operatorname{ord}_v j_E<0$).

Suppose that $v\mid p$ and E has additive potentially good reduction at v. Now apply Proposition 8.5(ii) for $p>3$, (iv) for $p=3$, and (v) for $p=2$ (noting that by class field theory, all upper ramification groups in the inertia group of $\mathrm{Gal}(K_\infty/K)=\mathbb{Z}_l$ are of finite index) to find that

$$\operatorname{ord}_p(\gamma_{v,n}^{n_{v,n}}) = \left(f_{K_v/\mathbb{Q}_p}\frac{\delta'-\delta}{12}e_{v,n}f_{v,n} + \epsilon_{v,n}f_{v,n}f_{K_v/\mathbb{Q}_p} + z_n\right)n_{v,n} = \mu_v l^n + O(1). \qquad \square$$

Corollary 8.8. *Theorem 1.2 holds.*

Proof. Combine Theorem 8.7 and Corollary 7.2. $\square$

Theorem 8.9. *Suppose that K is a number field and K_∞/K a Galois extension whose Galois group is a d-dimensional l-adic Lie group; write K_n/K for its nth layer in the natural Lie filtration. Let p be a prime number and $\phi: A\to A'$ a K-isogeny of abelian varieties. If either A and A' are semistable or they are elliptic curves that do not have additive potentially supersingular reduction at primes $v\,|\,p$ that are infinitely ramified in K_∞/K, then there are constants $\mu_1,\ldots,\mu_d\in\mathbb{Q}$ such that for all sufficiently large n,*

$$\begin{aligned}&\frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K_n)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A'^t/K_n)[\phi^t]|}\frac{|\text{Ш}^\circ_{A/K_n}[p^\infty]|}{|\text{Ш}^\circ_{A'/K_n}[p^\infty]|}\frac{|A'(K_n)[p^\infty]|\,|A'^t(K_n)[p^\infty]|}{|A(K_n)[p^\infty]|\,|A^t(K_n)[p^\infty]|}\\ &\quad = p^{\mu l^{dn}+\mu_1 l^{(d-1)n}+\cdots+\mu_{d-1}l^n+\mu_d}.\end{aligned}$$

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

If A is a general elliptic curve, then there is $\mu \in \mathbb{Q}$ such that for all sufficiently large n,

$$\frac{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A/K_n)[\phi]|}{|\mathrm{Sel}^{\mathrm{div}}_{p^\infty}(A'/K_n)[\phi^t]|}\frac{|Ш^{\circ}_{A/K_n}[p^\infty]|}{|Ш^{\circ}_{A'/K_n}[p^\infty]|} = p^{\mu l^{dn}+O(l^{(d-1)n})}.$$

Proof. We will apply Theorem 8.2. Note that the torsion contribution is $O(1)$ by Proposition 6.1, so we can ignore it for the second claim.

Fix a prime v of K. The decomposition group D_v and the inertia group I_v are closed Lie subgroups. So, for all sufficiently large n,

$$\begin{aligned} e_{v,n} &= C_1 l^{n(\dim I_v)}, \\ f_{v,n} &= C_2 l^{n(\dim D_v - \dim I_v)}, \\ n_{v,n} &= C_3 l^{n(d-\dim D_v)} \end{aligned}$$

for some constants C_1, C_2 and C_3 (that depend on v). If $v \nmid l$, then the tower K_∞/K_n is eventually tamely ramified at v, and $\dim I_v \leqslant 1$. If $v \mid l$, then, on the contrary, all the upper ramification subgroups of I_v are of finite index by Sen's theorem [Sen72, § 4, main theorem].

We now compute $\mathrm{ord}_p(\gamma_{v,n}^{n_{v,n}})$ for every place v of K.

- *v is Archimedean.* If v is real and stays real in the tower, or if v is complex, then $\gamma_{v,n} = 1$. Otherwise, $\gamma_{v,n} \in \mathbb{Q}$ stabilises for large enough n, so $\mathrm{ord}_p(\gamma_{v,n}^{n_{v,n}})$ grows like Cl^{dn} for a suitable $C \in \mathbb{Q}$.
- *$v \nmid p$ or A/K_v is semistable or A/K_v is an elliptic curve that is not additive potentially supersingular.* Again, $\mathrm{ord}_p\,\gamma_{v,n}$ is constant for large n, by Proposition 8.5(i), so $\mathrm{ord}_p(\gamma_{v,n}^{n_{v,n}})$ grows like $Cl^{n(d-\dim D_v)}$ for some $C \in \mathbb{Q}$.
- *$v \mid p$ and A/K_v is an elliptic curve.* By Proposition 8.5, for large n,

$$\mathrm{ord}_p\,\gamma_{v,n} = \mu_v e_{v,n} f_{v,n} + \epsilon_{v,n} f_{v,n} f_{K_v/\mathbb{Q}_p} + z_n,$$

  with z_n, μ_v and $\epsilon_{v,n}$ as in the proposition. (The proposition applies because either $v \mid l$ and the upper ramification groups at v have finite index in I_v, or $v \nmid l$ and K_∞/K_n are eventually tamely ramified.) If $e_{v,n} \to \infty$, then $\dim I_v \geqslant 1$ and $\mathrm{ord}_p(\gamma_{v,n}^{n_{v,n}}) = Cl^{dn} + O(l^{(d-1)n})$ for some $C \in \mathbb{Q}$. Otherwise, $e_{v,n}$ is eventually constant, as are z_n and $\epsilon_{v,n}$ by Remark 8.6. In that case, $\mathrm{ord}_p(\gamma_{v,n}^{n_{v,n}}) = Cl^{dn} + C' l^{n(d-\dim D_v)}$ for some $C, C' \in \mathbb{Q}$.

Taking the product over all places v and applying Theorem 8.2, we get the claim. (The term $(\Omega_{A'/K}/\Omega_{A/K})^{[K_n:K]}$ gives a contribution of the form $p^{Cl^{dn}}$ for some $C \in \mathbb{Q}$.) □

COROLLARY 8.10. *Theorem 1.3 holds.*

Proof. (i) This is Theorem 8.9(ii).

(ii) Combine Theorem 8.9(i) and Proposition 6.1.

(iii) If $\mathrm{rk}_p\, A/K_n = O(l^{(d-1)n})$, then the divisible Selmer quotient is $p^{O(l^{(d-1)n})}$ by Corollary 7.2, and the torsion quotient is $p^{O(1)}$ by Proposition 6.1. Moreover, if $\mathrm{rk}_p\, A/K_n$ and $A(K_n)[p^\infty]$ are bounded, then the torsion quotients stabilise by Proposition 6.1, as does the divisible Selmer quotient by Theorem 7.4(ii) applied to ϕ and to ϕ^t. This gives the results for $Ш^{\circ}$. □

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

Acknowledgements
This investigation was inspired by conversations with John Coates. We would like to thank him and also Masato Kurihara, Ralph Greenberg, Karl Rubin and Chris Wuthrich for their comments. The second author would like to thank Emmanuel College, Cambridge, where he was based while carrying out this research.

Both authors were supported by Royal Society University Research Fellowships.

Appendix. Conductors of elliptic curves in extensions

In this Appendix we give bounds on the growth of conductors of elliptic curves in extensions of local fields. These results are independent of the rest of the paper, and do not rely on the presence of an isogeny.

Let $\mathcal{K}$ be a finite extension of $\mathbb{Q}_l$, and let $I_{\mathcal{K}}$ be the inertia subgroup of $\mathrm{Gal}(\bar{\mathcal{K}}/\mathcal{K})$. We will be interested in continuous representations $\chi : I_{\mathcal{K}} \to \mathrm{GL}_d(\mathbb{C})$, in other words, those that factor through a finite extension of $\mathcal{K}$. We write I^n for the upper ramification groups of $I_{\mathcal{K}}$. We denote by $f_\chi, f_E, \ldots$ the conductor exponents of a representation, an elliptic curve, etc.

Notation A.1. For an irreducible continuous representation $\chi \neq \mathbf{1}$ of $I_{\mathcal{K}}$, set

$$m_\chi = \max_{i \geqslant 1}\{i : \chi(I^i) \neq \mathrm{id}\}.$$

We set $m_{\mathbf{1}} = -1$.

Lemma A.2. *Let χ and ρ be irreducible continuous representations of $I_{\mathcal{K}}$.*

(i) $m_\chi = f_\chi/\dim\chi - 1$.
(ii) *χ factors through $I_{\mathcal{K}}/I^n$ if and only if $m_\chi < n$.*
(iii) *If $m_\rho < m_\chi$, then $f_{\rho\otimes\chi} = f_\chi \dim\rho$.*
(iv) *If $m_\rho = m_\chi$, then $f_{\rho\otimes\chi} \leqslant f_\chi \dim\rho = f_\rho \dim\chi$.*

Proof. (i) See [Ser79, ch. 6, § 2, Exercise 2]. (This is formulated in [Ser79] on the level of finite extensions, but the definition extends directly to the whole of $I_{\mathcal{K}}$, since upper ramification groups behave well under quotients.)

(ii) This is clear.

(iii) By (ii), the group I^{m_χ} acts trivially on ρ and non-trivially on χ. As $I^{m_\chi} \lhd I_K$ and χ is irreducible, χ has no invariants under I^{m_χ}. Therefore $\rho\otimes\chi$ has no invariants either, and so each irreducible constituent τ of $\rho\otimes\chi$ has $m_\tau \geqslant m_\chi$. On the other hand, clearly I^m acts trivially on $\rho\otimes\chi$ for $m > m_\chi$, so $m_\tau = m_\chi$ and $f_\tau = (f_\chi/\dim\chi)\dim\tau$ by (i). Taking the sum over τ, we deduce that

$$f_{\rho\otimes\chi} = f_\chi \frac{\dim(\chi\otimes\rho)}{\dim\chi} = f_\chi \dim\rho.$$

(iv) As in (iii), let τ be an irreducible constituent of $\rho\otimes\chi$. For $m > m_\chi$, the group I^m acts trivially on χ and on ρ, and hence on τ. Therefore, by (ii), $m_\tau < m$, and taking the limit $m \to m_\chi$ gives $m_\tau \leqslant m_\chi$. By (i), $f_\tau \leqslant (f_\chi/\dim\chi)\dim\tau$, and taking the sum over τ as in (iii) gives the claim. □

Theorem A.3. *Let $\mathcal{K}$ be an l-adic field and $\rho : I_{\mathcal{K}} \to \mathrm{GL}_d(\mathbb{C})$ a non-trivial continuous irreducible representation. Take $n > f_\rho/\dim\rho - 1$, and write $N = I^n$ for the nth ramification subgroup (in the upper numbering) of $I_{\mathcal{K}}$. Then, for every finite extension $\mathcal{F}/\mathcal{K}$,*

$$f_{\mathrm{Res}_{\mathcal{F}}\rho} = f_{\mathrm{Res}_{\mathcal{F}^N}\rho} \leqslant e_{\mathcal{F}^N/\mathcal{K}}(f_\rho - d) + d.$$

Proof. Because conductors and the upper numbering remain unchanged in unramified extensions, we may assume that $\mathcal{F}/\mathcal{K}$ is totally ramified. Decompose $\mathrm{Ind}_{\mathcal{F}/\mathcal{K}} \mathbf{1}$ as $\bigoplus_{\tau\in J}\tau$ with τ irreducible. By the conductor-discriminant formula,

$$\begin{aligned} f_{\mathrm{Res}_{\mathcal{F}}\,\rho} &= f_{\mathrm{Ind}_{\mathcal{F}/\mathcal{K}}\mathrm{Res}_{\mathcal{F}}\,\rho} - d\, v_{\mathcal{K}}(\Delta_{\mathcal{F}/\mathcal{K}}) \\ &= f_{\rho\otimes\mathrm{Ind}_{\mathcal{F}/\mathcal{K}}\mathbf{1}} - d\, f_{\mathrm{Ind}_{\mathcal{F}/\mathcal{K}}\mathbf{1}} = \sum_{\tau\in J} f_{\rho\otimes\tau} - d\, f_\tau. \end{aligned}$$

Let $J_N \subset J$ be the (multi-)set of τ which factor through $I_{\mathcal{K}}/N$. Then

$$f_{\mathrm{Res}_{\mathcal{F}^N}\,\rho} = \sum_{\tau\in J_N} f_{\rho\otimes\tau} - d\, f_\tau$$

by the same argument. However, $m_\tau \geqslant n > m_\rho$ for $\tau \notin J_N$ by Lemma A.2(ii), and so the terms $f_{\rho\otimes\tau} - d\, f_\tau$ are 0 by Lemma A.2(iii) for such τ. This proves the equality $f_{\mathrm{Res}_{\mathcal{F}}\,\rho} = f_{\mathrm{Res}_{\mathcal{F}^N}\,\rho}$.

For the inequality, first observe that by the argument above,

$$f_{\mathrm{Res}_{\mathcal{F}}\,\rho} = \sum_{J_\rho}(f_{\rho\otimes\tau} - d\, f_\tau),$$

where $J_\rho \subset J_N$ is the set of $\tau \in J$ for which $m_\tau \leqslant m_\rho$. By Lemma A.2(iii) and (iv), noting that $\dim\tau \leqslant f_\tau$ for every $\tau \neq \mathbf{1}$, we have

$$\begin{aligned} f_{\mathrm{Res}_{\mathcal{F}}\,\rho} &= \sum_{\tau\in J_\rho}(f_{\rho\otimes\tau} - d\, f_\tau) \leqslant \sum_{\tau\in J_\rho}(f_\rho \dim\tau - d\, f_\tau) \\ &\leqslant f_\rho + \sum_{\tau\in J_\rho\setminus\{\mathbf{1}\}}(f_\rho\dim\tau - d\dim\tau) \\ &= f_\rho + (f_\rho - d)\biggl(\biggl(\sum_{\tau\in J_\rho}\dim\tau\biggr) - 1\biggr) \\ &\leqslant f_\rho + (f_\rho - d)\biggl(\biggl(\sum_{\tau\in J_N}\dim\tau\biggr) - 1\biggr) \\ &= f_\rho + (f_\rho - d)([\mathcal{F}^N : \mathcal{K}] - 1) = d + (f_\rho - d)[\mathcal{F}^N : \mathcal{K}], \end{aligned}$$

which gives the claim, as we assumed that $\mathcal{F}/\mathcal{K}$ is totally ramified. $\square$

THEOREM A.4. *Let $\mathcal{K}$ be an l-adic field and $E/\mathcal{K}$ an elliptic curve with additive reduction. Take $n > f_E/2 - 1$ and write $N = I^n$ for the nth ramification subgroup (in the upper numbering) of $\mathrm{Gal}(\bar{\mathcal{K}}/\mathcal{K})$. Then, for every finite extension $\mathcal{F}/\mathcal{K}$,*

$$f_{E/\mathcal{F}} = f_{E/\mathcal{F}^N} \leqslant e_{\mathcal{F}^N/\mathcal{K}}(f_{E/\mathcal{K}} - 2) + 2.$$

Proof. Write $\mathcal{L} = \mathcal{F}^N$. Let V be the Weil–Deligne representation associated to the first étale cohomology of $E/\mathcal{K}$, and let ρ be its 'Weil part' (i.e. the semisimplification of $H^1_{\text{ét}}(E, \mathbb{Q}_\ell) \otimes \mathbb{C}$ for some $\ell \neq l$).

Either ρ is irreducible or it is a sum of two one-dimensional characters ψ_1 and ψ_2 of the same conductor (because $\psi_1\psi_2 = \det\rho$ is the cyclotomic character, which is unramified). The conductor depends only on the action of the inertia group, so, by applying Theorem A.3 either to ρ directly or to the ψ_i, we find that $f_{\mathrm{Res}_{\mathcal{F}}\,\rho} = f_{\mathrm{Res}_{\mathcal{L}}\,\rho}$.

Now, if $E/\mathcal{K}$ has potentially good reduction, then V is a Weil representatation and $f_E = f_\rho$, so the result follows from Theorem A.3. If $E/\mathcal{L}$ has multiplicative reduction, then $f_{E/\mathcal{F}} = f_{E/\mathcal{L}} = 1$, and the result again follows.

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press

Finally, suppose that $E/\mathcal{L}$ has additive potentially multiplicative reduction. By Theorem A.3,

$$f_{\mathrm{Res}_{\mathcal{F}}\,\rho} = f_{\mathrm{Res}_{\mathcal{L}}\,\rho} \leqslant e_{\mathcal{L}/\mathcal{K}}(f_\rho - 2) + 2.$$

Over any field where E has additive reduction, $f_E = f_\rho \geqslant 2$. This fact over $\mathcal{L}$, together with the formula, shows that $f_{\mathrm{Res}_{\mathcal{F}}\,\rho} \geqslant 2$; in particular, E has additive reduction over $\mathcal{F}$. Thus E has additive reduction over all three fields, and the formula then translates to the claim in the theorem. □

Corollary A.5. *Let $\mathcal{K}$ be an l-adic field and $\mathcal{K}^\infty/\mathcal{K}$ a possibly infinite Galois extension. Let $E/\mathcal{K}$ be an elliptic curve with additive reduction. Suppose that for some $n > f_E/2 - 1$, the upper ramification subgroup $I^n_{\mathcal{K}^\infty/\mathcal{K}}$ of the inertia group of $\mathcal{K}^\infty/\mathcal{K}$ has finite index e. Then, for every finite extension $\mathcal{L}$ of $\mathcal{K}$ in $\mathcal{K}^\infty$,*

$$f_{E/\mathcal{L}} \leqslant e(f_{E/\mathcal{K}} - 2) + 2.$$

Proof. This is clear, since $e_{\mathcal{L}^{I_n}/\mathcal{K}} = e_{\mathcal{L}^I/\mathcal{K}} \leqslant e$, where $I = I^n_{\mathcal{K}_\infty/\mathcal{K}}$. □

Corollary A.6. *Let $\mathcal{K}$ be an l-adic field and $\mathcal{K}^\infty/\mathcal{K}$ a Galois extension whose Galois group is an l-adic Lie group. Then there is a constant $C > 0$ such that every elliptic curve $E/\mathcal{K}$ has conductor exponent $f_{E/\mathcal{L}} \leqslant C$ over all finite extensions $\mathcal{L}$ of $\mathcal{K}$ in $\mathcal{K}^\infty$. Moreover, if $\mathcal{K}^\infty = \bigcup_m \mathcal{K}_m$ with $\mathcal{K}_m/\mathcal{K}$ finite Galois, then $f_{E/\mathcal{K}_m}$ stabilises as $m \to \infty$.*

Proof. This is clear for curves with good and multiplicative reduction. If $E/\mathcal{K}$ has additive reduction, by [Pap93, Theorem 1] the conductor exponent $f_{E/\mathcal{K}}$ is at most 2, $3v_{\mathcal{K}}(3) + 2$ or $6v_{\mathcal{K}}(2) + 2$ when $l \geqslant 5$, $l = 3$ or $l = 2$, respectively. By Sen's theorem [Sen72, § 4, main theorem], $I^n_{\mathcal{K}^\infty/\mathcal{K}} \lhd I_{\mathcal{K}^\infty/\mathcal{K}}$ is of finite index for every n, so the two claims follow from Corollary A.5 and Theorem A.4. □

References

BD14 A. Betts and V. Dokchitser, *Finite quotients of $\mathbb{Z}[C_n]$-lattices and Tamagawa numbers of semistable abelian varieties*, Preprint (2014), arXiv:1405.3151.

BCP97 W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.

Cas65 J. W. S. Cassels, *Arithmetic on curves of genus* 1*. VIII: On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199.

CFKSV05 J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes Études Sci. **101** (2005), 163–208.

CS12 J. Coates and R. Sujatha, *On the $\mathcal{M}_H(G)$-conjecture*, in *Non-abelian fundamental groups and Iwasawa theory*, London Mathematical Society Lecture Note Series, vol. 393 (Cambridge University Press, Cambridge, 2012), 132–161.

DD06 T. Dokchitser and V. Dokchitser, *Computations in non-commutative Iwasawa theory, with an appendix by J. Coates and R. Sujatha*, Proc. Lond. Math. Soc. (3) **94** (2006), 211–272.

DD10 T. Dokchitser and V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), 567–596.

DD11 T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64.

DD13 T. Dokchitser and V. Dokchitser, *A remark on Tate's algorithm and Kodaira types*, Acta Arith. **160** (2013), 95–100.

DD15 T. Dokchitser and V. Dokchitser, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), 4339–4358.

Dri03 M. Drinen, *Iwasawa μ-invariants of elliptic curves and their symmetric powers*, J. Number Theory **102** (2003), 191–213.

Gre99 R. Greenberg, *Iwasawa theory for elliptic curves*, in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, Lecture Notes in Mathematics, vol. 1716 (Springer, Berlin, 1999), 51–144.

Gre01 R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*, in *Arithmetic algebraic geometry*, IAS/Park City Mathematics Series, vol. 9, eds B. Conrad *et al.* (2001), 407–464.

HM99 Y. Hachimori and K. Matsuno, *An analogue of Kida's formula for Selmer groups of elliptic curves*, J. Algebraic Geom. **8** (1999), 581–601.

HV03 Y. Hachimori and O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Doc. Math. (2003), 443–478; Extra volume: Kazuya Kato's fiftieth birthday.

Kat04 K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in *Cohomologies p-adique et applications arithmetiques III*, Asterisque, vol. 295 (2004), 117–290.

KT82 K. Kramer and J. Tunnell, *Elliptic curves and local ϵ-factors*, Compos. Math. **46** (1982), 307–352.

Kra90 A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), 353–385.

Kur02 M. Kurihara, *On the Tate–Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I*, Invent. Math. **149** (2002), 195–224.

Lam J. Lamplugh, *An analogue of the Washington–Sinnott theorem for elliptic curves with complex multiplication I*, J. Lond. Math. Soc. (2), to appear.

LRS93 P. Lockhart, M. Rosen and J. Silverman, *An upper bound for the conductor of an abelian variety*, J. Algebraic Geom. **2** (1993), 569–601.

Pap93 I. Papadopolous, *Sur la classification de Néron des courbes elliptiques*, J. Number Theory **44** (1993), 119–152.

Per87 B. Perrin-Riou, *Fonctions L p-adique, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), 399–456.

Rib81 K. A. Ribet, *Torsion points of abelian varieties in cyclotomic extensions, Appendix to N. M. Katz and S. Lang, Finiteness theorems in geometric class field theory*, L'Enseign. Math. **27** (1981), 315–319.

Sch87 P. Schneider, *The μ-invariant of isogenies*, J. Indian Math. Soc. (N.S.) **52** (1987), 159–170.

Sen72 S. Sen, *Ramification in p-adic Lie extensions*, Invent. Math. **17** (1972), 44–50.

Ser72 J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

Ser79 J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67 (Springer, New York, 1979).

Sil86 J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106 (Springer, New York, 1986).

Sil94 J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151 (Springer, New York, 1994).

Tat65/66 J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, *Séminaire Bourbaki*, 18e année, 1965/66, no. 306.

Was78 L. Washington, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*, Invent. Math. **49** (1978), 87–97.

Tim Dokchitser tim.dokchitser@bristol.ac.uk
Department of Mathematics, University of Bristol,
University Walk, Bristol BS8 1TW, UK

Vladimir Dokchitser v.dokchitser@warwick.ac.uk
Mathematics Institute, University of Warwick,
Coventry CV4 7AL, UK

https://doi.org/10.1112/S0010437X15007423 Published online by Cambridge University Press