PURSUING POLYNOMIAL BOUNDS ON TORSION

PETE L. CLARK AND PAUL POLLACK

ABSTRACT. We show that for all $\epsilon > 0$, there is a constant $C(\epsilon) > 0$ such that for all elliptic curves E defined over a number field F with $j(E) \in \mathbb{Q}$ we have

$$\#E(F)[\mathrm{tors}] \leq C(\epsilon)[F : \mathbb{Q}]^{5/2+\epsilon}.$$

We pursue further bounds on the size of the torsion subgroup of an elliptic curve over a number field $E_{/F}$ that are polynomial in $[F : \mathbb{Q}]$ under restrictions on $j(E)$. We give an unconditional result for $j(E)$ lying in a fixed quadratic field that is not imaginary of class number one as well as two further results, one conditional on GRH and one conditional on the strong boundedness of isogenies of prime degree for non-CM elliptic curves.

NOTATION

Let $\mathcal{P}$ be the set of prime numbers. For a commutative group G, we denote the subgroup of elements of order dividing n by $G[n]$ and the torsion subgroup – i.e., the subgroup of elements of finite order – by $G[\mathrm{tors}]$. For $\mathfrak{s} \subset \mathcal{P}$, we let $G[\mathfrak{s}^\infty]$ denote the subgroup of $G[\mathrm{tors}]$ of elements with order divisible only by primes in $\mathfrak{s}$. If for a commutative group G we have $G = G[n]$ for some $n \in \mathbb{Z}^+$ – as is the case if G is finite – then the least such n is the **exponent** $\exp G$ of G.

For a field F, let $\overline{F}$ be an algebraic closure. We denote by $\mathfrak{g}_F = \mathrm{Aut}(\overline{F}/F)$ the absolute Galois group of F. For $n \in \mathbb{Z}^+$ and a field F of characteristic 0, let $F(\mu_n)$ be the field obtained by adjoining to F the nth roots of unity, and let $F^{\mathrm{cyc}} = \bigcup_n F(\mu_n)$. Let $\chi_\ell \colon \mathfrak{g}_F \to \mathbb{Z}_\ell^\times$ be the ℓ-adic cyclotomic character, and put

$$F^{\ell\text{-cyc}} := \overline{F}^{\operatorname{Ker}\chi_\ell} = \bigcup_{n \in \mathbb{Z}^+} F(\mu_{\ell^n}).$$

1. INTRODUCTION

1.1. Known bounds on the torsion subgroup

For an elliptic curve E defined over a number field F, the torsion subgroup $E(F)[\mathrm{tors}]$ is finite. Moreover, by Merel's strong[1] uniform boundedness theorem [Me96], as we range over all degree d number fields F and all elliptic curves $E_{/F}$, we have

$$T(d) = \sup \#E(F)[\mathrm{tors}] < \infty.$$

Merel's work gives an explicit upper bound on $T(d)$, which was improved by Oesterlé (unpublished, but see [De16]) and Parent [Pa99]. These lie more than an exponential

Date: May 12, 2017.

[1]Here and throughout this paper we use the term "strong" to mean a bound that is uniform across elliptic curves defined over number fields of any fixed degree.

away from the best known lower bound, due to Breuer [Br10]:

$$\inf_d \frac{T(d)}{d \log\log d} > 0.$$

Various authors have conjectured that Breuer's lower bound is esentially sharp.

Conjecture 1.1. *We have* $T(d) = O(d \log\log d)$.

The following weaker conjecture is more widely believed.

Conjecture 1.2. $T(d)$ *is* polynomially bounded*: there is* $B > 1$ *such that*

$$T(d) = O(d^B).$$

Even Conjecture 1.2 seems to lie out of current reach. Since the work of Merel, Osterlé and Parent, progress on understanding the asymptotic behavior of $T(d)$ has come (only) by restricting the class of elliptic curves under consideration. For instance if we restrict to the case in which E has *complex multiplication* (CM) – and write $T_{\mathrm{CM}}(d)$ in place of $T(d)$ when this restriction is made – breakthrough work of Silverberg [Si88, Si92] gave the asymptotically correct upper bound on the exponent, and recent work by the present authors [CP15, CP17] shows

$$\limsup_d \frac{T_{\mathrm{CM}}(d)}{d \log\log d} = \frac{e^\gamma \pi}{\sqrt{3}}.$$

If we instead restrict to the class of elliptic curves with *integral moduli* – i.e., with j-invariant lying in the ring $\overline{\mathbb{Z}}$ of algebraic integers – and write $T_{\mathrm{IM}}(d)$ in place of $T(d)$, then Hindry-Silverman showed [HS99]

$$T_{\mathrm{IM}}(d) = O(d \log d).$$

1.2. **In pursuit of polynomial bounds**

In this paper we will pursue polynomial bounds on the size of the torsion subgroup in a different kind of restricted regime. We begin by stating the following result, which conveys the flavor with a minimum of technical hypotheses.

Theorem 1.3. *Let* $\epsilon > 0$. *Then there is* $C = C(\epsilon)$ *such that: for all degree* d *number fields* F *and all elliptic curves* $E_{/F}$ *arising via base extension from an elliptic curve* $(E_0)_{/\mathbb{Q}}$, *we have*

$$\exp E(F)[\mathrm{tors}] \leq C d^{3/2+\epsilon}. \tag{1.1}$$

Now we make some comments:

- Of course we can assume that E does not have CM.
- For any elliptic curve E over a number field F, we have

$$\#E(F)[\mathrm{tors}] \mid (\exp E(F)[\mathrm{tors}])^2. \tag{1.2}$$

  Thus, Theorem 1.3 implies a bound of $O_\epsilon(d^{3+\epsilon})$ on the size of the torsion subgroup itself. Later we will give an improvement of this bound.
- An easy quadratic twisting argument allows us to establish the bound (1.1) as we range over all elliptic curves $E_{/F}$ with $j(E) \in \mathbb{Q}$. This serves to motivate the type of further result we would like to prove.

Let $d_0 \in \mathbb{Z}^+$. For a positive integer d that is divisible by d_0, let $T_{d_0}(d)$ be the supremum of $\#E(F)[\mathrm{tors}]$ as E ranges over all elliptic curves defined over a degree d number field F such that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$.

Conjecture 1.4. *For each $d_0 \in \mathbb{Z}^+$, there are $B = B(d_0)$ and $C = C(d_0)$ such that*

$$T_{d_0}(d) \leq Cd^B.$$

Theorem 1.3 gives the case $d_0 = 1$ of Conjecture 1.4. At present we cannot prove Conjecture 1.4 unconditionally for any $d_0 \geq 2$, but we can make some progress in this direction, as shown by the following results.

Theorem 1.5. *Let F_0 be a quadratic number field that is not imaginary quadratic of class number one. (Thus, the discriminant of F_0 is not one of $-3, -4, -7, -8, -11, -19, -43, -67, -163$.) Then for all $\epsilon > 0$, there is $C = C(\epsilon, F_0)$ such that if F is a degree d number field and $E_{/F}$ is an elliptic curve with $j(E) \in F_0$, we have*

$$\exp E(F)[\text{tors}] \leq Cd^{3/2+\epsilon} \quad \textit{and} \quad \#E(F)[\text{tors}] \leq Cd^{5/2+\epsilon}.$$

Theorem 1.6. *Assume the Generalized Riemann Hypothesis (GRH).*[2] *Let F_0 be a number field that does not contain the Hilbert class field of any imaginary quadratic field. Then for all $\epsilon > 0$, there is $C = C(\epsilon, F_0)$ such that if F is a degree d number field and $E_{/F}$ is an elliptic curve with $j(E) \in F_0$, we have*

$$\exp E(F)[\text{tors}] \leq Cd^{3/2+\epsilon} \quad \textit{and} \quad \#E(F)[\text{tors}] \leq Cd^{5/2+\epsilon}.$$

For $d_0 \in \mathbb{Z}^+$, we introduce a hypothesis $\mathrm{SI}(d_0)$ defined as follows.

$\mathrm{SI}(d_0)$: There is prime $\ell_0 = \ell_0(d_0)$ such that for all primes $\ell > \ell_0$, the modular curve $X_0(\ell)$ has no noncuspidal non-CM points of degree d_0.

Theorem 1.7. *If $\mathrm{SI}(d_0)$ holds, then for all $\epsilon > 0$, there is $C = C(\epsilon, d_0)$ with*

$$T_{d_0}(d) \leq Cd^{\frac{5}{2}+\epsilon}.$$

Remark 1.8. This paper is cognate to another work [CMP17], written in parallel, giving "typical bounds" on $\#E(F)[\text{tors}]$ for an elliptic curve $E_{/F}$, under the same hypotheses as Theorems 1.5, 1.6 and 1.7.

1.3. **Strategy of the proofs**

In [Ar08], Arai showed that for each fixed prime ℓ and number field F, as we range over all non-CM elliptic curves $E_{/F}$ there is a uniform upper bound on the index of the image of the ℓ-adic Galois representation. In §2 we prove the *strong* form of this theorem by showing that the conclusion still holds as we range over all non-CM elliptic curves defined over all number fields of any fixed degree (Theorem 2.3).

A uniform upper bound on the index of the *adelic* Galois representation as we range over all non-CM elliptic curves defined over number fields of fixed degree d_0 would be – to say the least! – desirable. It implies $\mathrm{SI}(d_0)$ but is so much stronger that the $d_0 = 1$ case was raised as an open problem in [Se72], has guided most subsequent work in the field, and remains open. Our approach to the ℓ-adic version exploits the finiteness properties that $\mathrm{GL}_2(\mathbb{Z}_\ell)$ enjoys by virtue of being an ℓ-adic analytic group – finiteness properties that $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ certainly does not possess.

From Theorem 2.3 we deduce Theorem 2.8: for each finite set of primes $\mathfrak{s}$, the quantity $\exp E(F)[\mathfrak{s}^\infty]$ is bounded by a polynomial in $[F : \mathbb{Q}(j(E))]$. Thus in order to bound $\exp E(F)[\text{tors}]$ it suffices to bound $\exp E(F)[\ell^\infty]$ for all *sufficiently large* primes.

The next ingredient is the following striking recent result.

[2]Throughout, we use GRH to mean the Riemann Hypothesis for all Dedekind zeta functions.

Theorem 1.9 (Lozano-Robledo). *Let $\ell > 2$ be a prime. Let F_0 be a number field, $\mathfrak{l}$ a prime ideal of $\mathbb{Z}_{F_0}$ lying over ℓ, and $e(\mathfrak{l}/\ell)$ the ramification index. Let $E_{/F_0}$ be a non-CM elliptic curve, and let $a \in \mathbb{Z}^+$ be such that E admits no F_0-rational cyclic isogeny of degree ℓ^a. Let $n \geq a$, and let $P \in E(\overline{F_0})$ have order ℓ^n. Then there is an integer $1 \leq c \leq 12e(\mathfrak{l}/\ell)$ and a prime $\mathcal{L}$ of $F_0(P)$ lying over $\mathfrak{l}$ such that the ramification index $e(\mathcal{L}/\mathfrak{l})$ is divisible by either $\frac{\varphi(\ell^n)}{\gcd(\varphi(\ell^n), c\ell^{a-1})}$ or by ℓ^{n-a+1}.*

Proof. This is a simplified form of [LR15, Thm. 2.1]. □

To apply Theorem 1.9 to get uniform bounds on $\exp E(F)[\mathrm{tors}]$, we need finiteness results for rational ℓ-isogenies. Thus Hypothesis $\mathrm{SI}(d_0)$ intervenes naturally.

Corollary 1.10. *Let $d_0 \in \mathbb{Z}^+$, and assume hypothesis $\mathrm{SI}(d_0)$. There is a prime $\ell_0 = \ell_0(d_0)$ such that: for all number fields $F_0/\mathbb{Q}$ of degree d_0 and all primes $\ell > \ell_0$, if $\mathfrak{l}$ is a prime ideal of $\mathbb{Z}_{F_0}$ lying over ℓ and $E_{/F_0}$ is a non-CM elliptic curve, then for all $n \in \mathbb{Z}^+$, if $P \in E(\overline{F_0})$ is a point of order ℓ^n, then there is $1 \leq c \leq 12d_0$ and a prime $\mathcal{L}$ of $F_0(P)$ lying over $\mathfrak{l}$ such that $e(\mathcal{L}/\mathfrak{l})$ is divisible by either $\frac{\varphi(\ell^n)}{\gcd(\varphi(\ell^n), c)}$ or by ℓ^n.*

Proof. This follows from Theorem 1.9 and the bound $e(\mathfrak{l}/l) \leq d_0$. □

To proceed without assuming $\mathrm{SI}(d_0)$ we need to restrict to weaker statements that are known or conditionally known. We make use of the following prior results.

Theorem 1.11 (Mazur [Ma78]). *The hypothesis $\mathrm{SI}(1)$ holds with $\ell_0(1) = 37$.*

Theorems 1.7 and 1.11 imply Theorem 1.3.

Theorem 1.12 (Momose [Mo95]). *Let F_0 be a quadratic field that is not imaginary quadratic of class number 1. There is a prime number $\ell_0 = \ell_0(F_0)$ such that for all primes $\ell > \ell_0$, no elliptic curve $E_{/F_0}$ admits an F_0-rational isogeny of degree ℓ.*

Theorem 1.13 (Larson-Vaintrob [LV14, Cor. 6.5]). *Let F_0 be a number field that does not contain the Hilbert class field of any imaginary quadratic field. If the Generalized Riemann Hypothesis (GRH) holds, then the set of prime numbers ℓ such that some elliptic curve $E_{/F_0}$ admits an F_0-rational ℓ-isogeny is finite.*

Corollary 1.14. *Let F_0 be a number field that does not contain the Hilbert class field of any imaginary quadratic field. If $[F_0 : \mathbb{Q}] \geq 3$, assume GRH. Then there is a prime $\ell_0 = \ell_0(F_0)$ such that: for all primes $\ell > \ell_0$, if $\mathfrak{l}$ is a prime ideal of $\mathbb{Z}_{F_0}$ lying over ℓ, and $E_{/F_0}$ is an elliptic curve, then for all $n \in \mathbb{Z}^+$, if $P \in E(\overline{F_0})$ is a point of order ℓ^n, then there is an integer $1 \leq c \leq 12e(\mathfrak{l}/l)$ and a prime $\mathcal{L}$ of $F_0(P)$ lying over $\mathfrak{l}$ such that $e(\mathcal{L}/\mathfrak{l})$ is divisible by either $\frac{\varphi(\ell^n)}{\gcd(\varphi(\ell^n), c)}$ or by ℓ^n.*

Proof. Combine Theorems 1.9, 1.12 and 1.13. □

In §3.2 we use Corollaries 1.10 and 1.14 to get the polynomial bounds on $\exp E(F)[\mathrm{tors}]$ of Theorems 1.5, 1.6 and 1.7. Via (1.2) this immediately gives a polynomial bound on $\#E(F)[\mathrm{tors}]$. However in §3.3 we improve this bound using an analysis of cyclotomic characters, completing the proofs of Theorems 1.3, 1.5, 1.6 and 1.7.

2. Bounded index results for the ℓ-adic Galois representation

2.1. Statement of the strong Arai theorem

Let F be a number field, and let $E_{/F}$ be a non-CM elliptic curve. Let

$$\widehat{\rho}\colon \mathfrak{g}_F \to \operatorname{Aut} TE \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

denote the adelic Galois representation of $E_{/F}$, and for a prime ℓ, let

$$\rho_{\ell^\infty} : \mathfrak{g}_F \to \operatorname{Aut} T_\ell E \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$$

denote the ℓ-adic Galois representation of $E_{/F}$. Then $\det \rho_{\ell^\infty} = \chi_\ell$ and $F^{\ell\text{-cyc}} = \overline{F}^{\operatorname{Ker}\chi_\ell}$, so

$$\rho_{\ell^\infty}(\mathfrak{g}_{F^{\ell\text{-cyc}}}) = \rho_{\ell^\infty}(\mathfrak{g}_F) \cap \mathrm{SL}_2(\mathbb{Z}_\ell). \tag{2.1}$$

By a result of Serre [Se72], the image $\widehat{\rho}(\mathfrak{g}_F)$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ – equivalently, has finite index. Thus for each prime ℓ the ℓ-adic image $\rho_{\ell^\infty}(\mathfrak{g}_F)$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and ρ_{ℓ^∞} is surjective for all but finitely many primes ℓ. As mentioned above, a uniform adelic open image theorem is the *ultima Thule* of this field, but Arai has proved a uniform ℓ-adic open image theorem.

Theorem 2.1 (Arai [Ar08])**.** *Let F be a number field, and let ℓ be a prime. There is $I \in \mathbb{Z}^+$ such that for every non-CM elliptic curve $E_{/F}$, the image $\rho_{\ell^\infty}(\mathfrak{g}_F)$ of the ℓ-adic Galois representation has index at most I in $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

Remark 2.2. Arai states Theorem 2.1 slightly differently. For $n \in \mathbb{Z}^+$, put

$$\mathcal{U}^{(n)} := \operatorname{Ker}(\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})).$$

Then each $\mathcal{U}^{(n)}$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and each open subgroup Γ of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ contains $\mathcal{U}^{(n)}$ for all sufficiently large n. The least such n is called the **level** of Γ. Then Arai proves: for a number field F and a prime ℓ, there is $n = n(F,\ell)$ such that for every non-CM elliptic curve $E_{/F}$, the level of $\rho_{\ell^\infty}(\mathfrak{g}_F)$ is at most n.

The statement in terms of the level immediately implies the statement in terms of the index. The reverse implication holds because (cf. Lemma 2.5a)) the intersection of all open subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ of index at most I is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

The main goal of this section is to prove the following *strong* form of Arai's theorem.

Theorem 2.3. *Fix a prime number ℓ and a positive integer d.*

a) *As we range over all non-CM elliptic curves $E_{/F}$ defined over number fields of degree d, there is an absolute bound on the index of the image of the ℓ-adic Galois representation $\rho_{\ell^\infty}(\mathfrak{g}_F)$ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

b) *Moreover, for all but finitely many j-invariants we have*

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{\ell^\infty}(\mathfrak{g}_F)] \leq \frac{3200d^2}{7}.$$

Remark 2.4.

a) Theorem 2.3a) is a quick consequence of results of Cadoret and Tamagawa [CT12, CT13]. Namely, we apply [CT13, Thm. 1.1] with $k = \mathbb{Q}$ to the family of elliptic curves $E \to X := \mathbb{P}^1 \setminus \{0, 1728, \infty\}$ given by

$$E_j : y^2 + xy - x^3 + \frac{36}{j - 1728}x + \frac{1}{j - 1728} = 0$$

of [CT12, §5.1.3] – this family is geometrically Lie perfect by [CT12, Thm. 5.1]. The conclusion is that, for each $d \in \mathbb{Z}^+$, for each fixed prime ℓ and positive integer d, there is $B(\ell, d) \in \mathbb{Z}^+$ such that for all but finitely many closed points $j \in X$ of degree at most d, the index of the image of ℓ-adic Galois representation on $(E_j)_{/\mathbb{Q}(j)}$ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is at most $B(\ell, d)$. By Serre's open image theorem the result extends to all non-CM j-invariants of degree at most d with some absolute bound, say $\widetilde{B(\ell, d)}$. For any non-CM elliptic curve E defined over a degree d number field F, there is an elliptic curve E_j in the above family and a number field $K \supset F(j(E))$ with $[K : \mathbb{Q}] \leq 2d$ such that $(E_j)_{/K} \cong E_{/K}$. The index of the image of the ℓ-adic Galois representation of $E_{/F}$ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is no larger than the index of the ℓ-adic Galois representation of $E_{/K}$ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and thus no larger than $2d \cdot \widetilde{B(\ell, d)}$.

b) Rouse outlined a proof of Theorem 2.3a) on MathOverflow [R-MO]. His methods would yield a version of Theorem 2.3b).

c) Theorem 2.3a) is sufficient for our applications. Nevertheless we want to include a proof of Theorem 2.3b). First, it seems interesting that in a natural case[3] of [CT13, Thm. 1.1] we can get a bound that is – after omitting a finite set of j-invariants that depends on ℓ and d – explicit and independent of ℓ. Second, the proof of [CT13, Thm. 1.1] takes about 25 pages, whereas the outline of [R-MO] is 13 lines. Our argument is about 2.5 pages; readers may appreciate having a proof of this intermediate length. Finally, in [CT13, Thm. 1.2], Cadoret-Tamagawa state a result of Frey [Fr94] but omit Frey's assumption that $X(k) \neq \varnothing$. This is easily remedied by using a variant on Frey's result from [Cl09], and our argument shows how to do this.

2.2. **Group theoretic preliminaries**

Lemma 2.5. *Let ℓ be a prime, and let G be an infinite ℓ-adic analytic group.*

a) *G is topologically finitely generated. A subgroup of G is open iff it has finite index. For all $I \in \mathbb{Z}^+$, there are only finitely many index I subgroups of G.*

b) *Every open subgroup of G has at least one and finitely many maximal proper open subgroups.*

c) *Let $\mathcal{F}$ be a set of open subgroups of G such that $\mathcal{F}$ contains all but finitely many open subgroups of G. Then every element of $\mathcal{F}$ is contained in a maximal element, and $\mathcal{F}$ has finitely many maximal elements.*

d) *For $I \in \mathbb{Z}^+$, the family $\mathcal{F}_I$ of open subgroups $H \subset G$ with $[G : H] > I$ satisfies the hypotheses of part c) and thus has at least one and finitely many maximal elements.*

Proof. a) Lazard has shown that an ℓ-adic analytic group is topologically finitely generated and that a subgroup of G is open iff it has finite index [La65]. Moreover, every topologically finitely generated profinite group has only finitely many open subgroups of any given finite index [FJ, Lemma 16.10.2].[4]

b) Every nontrivial profinite group has a proper open subgroup, and any such group is contained in a maximal proper subgroup. And every open subgroup U of G is again

[3] In [CT12], the authors identify Arai's work as a motivation for their own.

[4] Each finite index subgroup of a topologically finitely generated profinite group is open [NS07].

an ℓ-adic analytic group, so by [S-LMW, pp. 148–149] the Frattini subgroup $\Phi(U)$ is open and thus U has only finitely many maximal proper open subgroups.

c) We may assume $G \notin \mathcal{F}$. Since G is infinite and profinite, $\mathcal{F} \neq \varnothing$. As for any group, the set of finite index subgroups of G, partially ordered under inclusion, satisfies the ascending chain condition, hence so does $\mathcal{F}$ and every element of $\mathcal{F}$ is contained in a maximal element. To show that there are only finitely many maximal elements of $\mathcal{F}$ it suffices to find a finite subset $\mathcal{S} \subset \mathcal{F}$ such that for every $K \in \mathcal{F}$ there is $H \in \mathcal{S}$ such that $K \subseteq H$, for then the maximal elements of $\mathcal{F}$ are the maximal elements of $\mathcal{S}$.

Let $\mathcal{S}$ be the set of elements $H \in \mathcal{F}$ such that H is a maximal proper open subgroup of an open subgroup P of G such that $P \notin \mathcal{F}$. By assumption the set of such subgroups P is finite, so $\mathcal{S}$ is finite by part b). Because $G \notin \mathcal{G}$, for $K \in \mathcal{F}$, the set of subgroups Q with $K \subsetneq Q \subseteq G$ and $Q \notin \mathcal{F}$ is finite and nonempty; choose a minimal element $\underline{Q}$. The set of subgroups H with $K \subseteq H \subsetneq \underline{Q}$ is finite and nonempty; choose a maximal element $\overline{H}$. Then $K \subset \overline{H}$ and $\overline{H} \in \mathcal{S}$. d) This is immediate from part a). □

Remark 2.6. It follows from [S-LMW, pp. 148] that the necessary and sufficient condition on a profinite group G for all of the conclusions of Lemma 2.5 to hold for G is that the Frattini subgroup $\Phi(G)$ of G be open.

Lemma 2.7. *Let F be a degree d number field, and let $E_{/F}$ be an elliptic curve. Let ℓ be a prime number. Let $G = \rho_{\ell^\infty}(\mathfrak{g}_F)$ be the image of the ℓ-adic Galois representation on E and let $H = G \cap \mathrm{SL}_2(\mathbb{Z}_\ell)$. Then we have*

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : G] \leq d[\mathrm{SL}_2(\mathbb{Z}_\ell) : H]. \tag{2.2}$$

Proof. Step 1: Let G be a group, let N be a normal subgroup of G, and let $q\colon G \to G/N$ be the quotient map. Then we have

$$[G : H] \leq [N : H \cap N][G/N : q(H)]. \tag{2.3}$$

Indeed, let $X \subset G$ have cardinality larger than $[N : H \cap N][G/N : q(H)]$. By the Pigeonhole Principle, there is $Y \subset X$ of cardinality larger than $[N : H \cap N] = [HN : H]$ such that for all $y_1, y_2 \in Y$, we have $q(y_2 y_1^{-1}) \in q(H)$, so $y_2 y_1^{-1} \in q^{-1}(q(H)) = HN$. So there are $y_1 \neq y_2$ such that $y_1 H = y_2 H$.

Step 2: The ℓ-adic cyclotomic character $\chi_\ell\colon \mathfrak{g}_{\mathbb{Q}} \to \widehat{\mathbb{Z}}_\ell^\times$ is surjective, so for any degree d number field F and elliptic curve $E_{/F}$, we have $[\mathbb{Z}_\ell^\times : \det \rho_{\ell^\infty}(\mathfrak{g}_F)] \mid d$. Applying (2.3) with $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$, $N = \mathrm{SL}_2(\mathbb{Z}_\ell)$, $H = G$ and using (2.1), we get (2.2). □

2.3. **Proof of Theorem 2.3**

Step 1: Put $I \coloneqq \lfloor 1600d^2/7 \rfloor$. Let F be a number field, let $E_{/F}$ be a non-CM elliptic curve, and let $G = \rho_{\ell^\infty}(\mathfrak{g}_F)$ be the image of the ℓ-adic Galois representation on $E_{/F}$. Some quadratic twist E' of E has $-1 \in G$. Put $G' \coloneqq \rho_{\ell^\infty}(\mathfrak{g}_F)$. Then $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G] \leq 2[\mathrm{GL}_2(\mathbb{Z}_\ell) : G']$, so it suffices to work with E'. We may also assume that $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G'] > I$. Applying Lemma 2.5 with $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$ we get that G' is contained in one of finitely many open subgroups $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}_\ell)$ with $[\mathrm{GL}_2(\mathbb{Z}_\ell) : \Gamma] > I$. So it suffices to bound $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G']$ while assuming that $G' \subset \Gamma$ for a *fixed* Γ.

Step 2: Let $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}_\ell)$ be an open subgroup with

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : \Gamma] > I. \tag{2.4}$$

Put

$$S\Gamma := \Gamma \cap \mathrm{SL}_2(\mathbb{Z}_\ell).$$

Then $\overline{\Gamma} := \Gamma \cap \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let $P\overline{\Gamma}$ be the image of $\overline{\Gamma}$ in $\mathrm{PSL}_2(\mathbb{Z})$, and put $D_\Gamma := [\mathrm{PSL}_2(\mathbb{Z}) : P\overline{\Gamma}]$. Since $-1 \in G' \subset \Gamma$, we have $[\mathrm{PSL}_2(\mathbb{Z}) : P\overline{\Gamma}] = [\mathrm{SL}_2(\mathbb{Z}) : S\Gamma]$. Using (2.2) we get

$$D_\Gamma \geq \frac{[\mathrm{GL}_2(\mathbb{Z}_\ell) : \Gamma]}{d}.$$

Step 3: Let $\mathbb{Q}(\Gamma)$ be the finite subextension of $\mathbb{Q}^{\ell\text{-cyc}}/\mathbb{Q}$ corresponding to the open subgroup $\det \Gamma \subset \mathbb{Z}_\ell^\times$. Then there is a modular curve X_Γ that is defined and geometrically integral over $\mathbb{Q}(\Gamma)$, and such that the base extension of X_Γ to $\mathbb{C}$ is the compact Riemann surface $\overline{\Gamma}\backslash\overline{\mathcal{H}}$. If for an elliptic curve $E_{/F}$ we have $G = \rho_{\ell^\infty}(\mathfrak{g}_F) \subset \langle \Gamma, -1 \rangle$, then $\mathbb{Q}(\Gamma) \subset F$, and there is an induced point on $X_\Gamma(F)$ and thus a closed point on X_Γ of degree dividing d. Let $\mathfrak{d}_\Gamma$ be the gonality of the curve X_Γ – the least positive degree of a map $X_\Gamma \to \mathbb{P}^1$ defined over $\mathbb{Q}(\Gamma)$ – and let $\overline{\mathfrak{d}}_\Gamma$ be the gonality of $(X_\Gamma)_{/\mathbb{C}}$, so

$$\overline{\mathfrak{d}}_\Gamma \leq \mathfrak{d}_\Gamma.$$

We claim that X_Γ has only finitely many closed points of degree dividing d. Indeed, if not then by [Cl09, Thm. 5] we have

$$\mathfrak{d}_\Gamma \leq 2d.$$

On the other hand, by a theorem of Abramovich [Ab96, Thm. 0.1], we have

$$\overline{\mathfrak{d}}_\Gamma \geq \frac{7}{800} D_\Gamma.$$

Putting these results together, we get the upper bound

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : \Gamma] \leq \frac{1600}{7} d^2,$$

and thus

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : \Gamma] \leq I,$$

contradicting (2.4). Thus the set of j-invariants of non-CM elliptic curves over degree d number fields such that the index of the image of the ℓ-adic Galois representation exceeds $\frac{3200}{7} d^2$ is finite. (Here we have multiplied by 2 to get back from G' to G.) Let the exceptional j-invariants be $j_1, \ldots, j_M \in \overline{\mathbb{Q}}$. For $1 \leq i \leq M$, choose an elliptic curve $E_{/\mathbb{Q}(j_i)}$ with j-invariant j_i, and let I_i be the index of the image of the ℓ-adic Galois representation (by Serre's open image theorem, each I_i is finite). Now let $E_{/F}$ be a non-CM elliptic curve defined over a degree d number field F such that the index of the image of the ℓ-adic Galois representation exceeds $\frac{3200}{7} d^2$. Then $j(E) = j(E_i)$ for some i. There is a number field $K \supset F$ such that $E_{/K} \cong (E_i)_{/K}$ and $[K : \mathbb{Q}] \leq 2d^2$, and thus the index of the image of the ℓ-adic Galois representation of $E_{/F}$ is at most $2d^2 I_i$. So for any non-CM elliptic curve over any degree d number field for which the image of the ℓ-adic Galois representation is contained in Γ, the index of the image of the ℓ-adic Galois representation is at most

$$\max\left(\frac{3200}{7} d^2, \max_{1 \leq i \leq M} 2d^2 I_i\right).$$

2.4. **A consequence**

Theorem 2.8. *Let $d_0 \in \mathbb{Z}^+$, and let $\mathfrak{s} \subset \mathcal{P}$ be finite. There is $C = C(d_0, \mathfrak{s}) \in \mathbb{Z}^+$ such that if $E_{/F}$ is a non-CM elliptic curve with $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$, then*

$$\exp E(F)[\mathfrak{s}^\infty] \leq C[F : \mathbb{Q}(j(E))]^{\frac{1}{2}}.$$

Proof. We consider non-CM elliptic curves E defined over number fields F such that $F_0 \coloneqq \mathbb{Q}(j(E))$ is a number field of degree d_0. In case $F = F_0$, as we range over all $E_{/F_0}$, by Theorem 2.3 the index of the image of the ℓ-adic Galois representation is uniformly bounded. Thus there is $v_\ell \in \mathbb{N}$ such that for all such $E_{/F_0}$, we have

$$\mathrm{ord}_\ell[\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E,\ell^\infty}(\mathfrak{g}_{F_0})] \leq v_\ell.$$

With this notation, we will show that we may take

$$C = \left(2\prod_{\ell \in \mathfrak{s}} \ell^{2+v_\ell}\right)^{\frac{1}{2}}.$$

Now let $E_{/F}$ be as above, and suppose $E(F)$ has a point of order

$$N = \prod_{\ell \in \mathfrak{s}} \ell^{a_\ell}.$$

Let $\mathfrak{s}' = \{\ell \in \mathfrak{s} \mid a_\ell > 0\}$. We also suppose, temporarily, that E arises by base extension from an elliptic curve defined over F_0. Let $\ell \in \mathfrak{s}'$. Since $E(F)$ has a point of order ℓ^{a_ℓ}, this forces the image of the ℓ-adic Galois representation to lie in a subgroup conjugate to

$$\Gamma_1(\ell^{a_\ell}) := \begin{bmatrix} 1 + \ell^{a_\ell}\mathbb{Z}_\ell & \mathbb{Z}_\ell \\ \ell^{a_\ell}\mathbb{Z}_\ell & \mathbb{Z}_\ell^\times \end{bmatrix}.$$

Since $[\mathrm{GL}_2(\mathbb{Z}_\ell) : \Gamma_1(\ell^{a_\ell})] = \ell^{2a_\ell - 2}(\ell^2 - 1)$, we get

$$\ell^{2a_\ell-2}(\ell^2-1) \mid [\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E,\ell^\infty}(\mathfrak{g}_F)] \mid [F : F_0][\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E,\ell^\infty}(\mathfrak{g}_{F_0})]$$

and thus

$$\ell^{2a_\ell-2-v_\ell} \mid [F : F_0].$$

(Here and below, we write $a \mid b$ for rational numbers a, b whenever $b = aq$ for some $q \in \mathbb{Z}$.) Compiling these divisibilities across all $\ell \in \mathfrak{s}'$, we get

$$\frac{N^2}{\prod_{\ell \in \mathfrak{s}'} \ell^{2+v_\ell}} \mid [F : F_0]$$

and thus

$$N \leq \left(\prod_{\ell \in \mathfrak{s}'} \ell^{2+v_\ell}\right)^{\frac{1}{2}} [F : F_0]^{\frac{1}{2}} \leq \left(\prod_{\ell \in \mathfrak{s}} \ell^{2+v_\ell}\right)^{\frac{1}{2}} [F : F_0]^{\frac{1}{2}}.$$

Now suppose that $E_{/F}$ does not necessarily arise by base extension from an elliptic curve over F_0. Nevertheless there is an elliptic curve $(E_0)_{/F_0}$ and and a quadratic extension F'/F such that $E_{/F'} \cong (E_0)_{/F'}$. Since $\exp E(F)[\mathfrak{s}^\infty] \mid \exp E(F')[\mathfrak{s}^\infty]$, applying the previously addressed special case with F' in place of F gives

$$N \leq \left(\prod_{\ell \in \mathfrak{s}} \ell^{2+v_\ell}\right)^{\frac{1}{2}} [F' : F_0]^{\frac{1}{2}} = \left(2\prod_{\ell \in \mathfrak{s}} \ell^{2+v_\ell}\right)^{\frac{1}{2}} [F : F_0]^{\frac{1}{2}}. \qquad \square$$

Remark 2.9. Theorem 2.8 is sharp up to the value of the constant. Indeed, for a non-CM elliptic curve E defined over a number field F_0 and any prime ℓ, since there are $(\ell^2-1)\ell^{2n-2}$ points of order ℓ^n on $E(\overline{F})$, there is a field extension F_n/F_0 of degree at most $(\ell^2-1)\ell^{2n-2} < \ell^{2n}$ such that $E(F_n)$ has a point of order ℓ^n.

3. The proofs of Theorems 1.5, 1.6 and 1.7

3.1. **An easy lemma**

Lemma 3.1. *Let F be a complete discretely valued field, with residue characteristic $p \geq 0$. Let $\ell \neq p$ be a prime number, and let $E_{/F}$ be an elliptic curve over F with semistable reduction. Then $e(F(E[\ell])/F) \mid \ell$.*

Proof. Case 1: Suppose $E_{/F}$ has good reduction. Then by the Néron-Ogg-Shafarevich criterion, since $\ell \neq p$ the extension $F(E[\ell])/F$ is unramified: $e(F(E[\ell])/F) = 1$.

Case 2: Suppose $E_{/F}$ has multiplicative reduction. Then there is an unramified quadratic extension F'/F such that $E_{/F'}$ admits an analytic uniformization, or in other words is a **Tate curve** in the sense of [Si94, §5.3]: $E_{/F'} \cong \mathbb{G}_m/\langle q^{\mathbb{Z}}\rangle$. It follows that $F'(E[\ell]) = F'(\mu_\ell, q^{\frac{1}{\ell}})$. Put $F'' = F'(\mu_\ell)$. Since F'/F is unramified and $\ell \neq p$, the extension $F''(q^{\frac{1}{\ell}})/F''$ is Galois and

$$e(F(E[\ell])/F) = e(F''(q^{\frac{1}{\ell}})/F'') \mid [F''(q^{\frac{1}{\ell}}) : F''].$$

By Kummer theory, we have

$$[F''(q^{\frac{1}{\ell}}) : F''] = \begin{cases} 1 & \text{if } q \text{ is an } \ell\text{th power in } F'', \\ \ell & \text{otherwise.} \end{cases}$$ □

3.2. **Bounding the exponent**

For the sake of a uniform presentation, we begin by fixing some notation. In the case of Theorems 1.5 and 1.6, we let F_0 be as in the theorem statement, put $d_0 = [F_0 : \mathbb{Q}]$, and define ℓ_0 as in Corollary 1.14. In the case of Theorem 1.7, we let F_0 be any number field of the given degree d_0, and we define ℓ_0 as in Corollary 1.10.

Let E be a non-CM elliptic curve over over a degree d number field F having $j(E) \in F_0$. (For CM curves, any of [Si92], [HS99], [CP15, CP17] yield stronger results.) It suffices to show that there is a constant C with

$$\exp E(F)[\text{tors}] \leq Cd^{3/2+\epsilon},$$

where C is a function of ℓ_0, d_0, and ϵ. Note that since ℓ_0 is determined by F_0 in the case of Theorems 1.5 and 1.6, the constant C depends on F_0 and ϵ in those theorems. Since ℓ_0 is determined by d_0 in the case of Theorem 1.7, the constant C depends only on d_0 and ϵ in that situation.

Step 0: We first reduce to a special case. Suppose that there is a $C' > 0$ with the property that for all elliptic curves $E_{/F}$ obtained by base extension from an elliptic curve $(E_0)_{/F_0}$, we have

$$\exp E(F)[\text{tors}] \leq C'[F : \mathbb{Q}]^{3/2+\epsilon}.$$

Now let $E_{/F}$ be an elliptic curve with $j(E) \in F_0$. Then there is an elliptic curve $(E_0)_{/F_0}$ with $j(E) = j(E_0)$ and a quadratic extension F'/F such that $E_{/F'} \cong (E_0)_{/F'}$.

Let $d = [F : \mathbb{Q}]$ and $d' = [F' : \mathbb{Q}]$. Then

$$\exp E(F)[\text{tors}] \mid \exp E(F')[\text{tors}] \leq C' \cdot d'^{3/2+\epsilon} \leq (C' \cdot 2^{3/2+\epsilon}) \cdot d^{3/2+\epsilon}.$$

So we may choose $C = C' \cdot 2^{3/2+\epsilon}$. If C' depends only on ℓ_0, d_0, and ϵ, then so does C.

Step 1: Now suppose that E is obtained by base change from an elliptic curve defined over F_0, which for notational simplicity we continue to denote by E. Write

$$E(F)[\text{tors}] = \prod_{\ell \in \mathcal{P}} E(F)[\ell^\infty]$$

and, for $\ell \in \mathcal{P}$,

$$E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^{a_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{b_\ell}\mathbb{Z}$$

for integers a_ℓ, b_ℓ satisfying $0 \leq a_\ell \leq b_\ell$. We will partition $\{\ell \in \mathcal{P} \mid b_\ell \geq 1\}$ into two classes $\mathcal{S}_1$ and $\mathcal{S}_2$, get bounds on $\exp E(F)[\mathcal{S}_1^\infty]$ and $\exp E(F)[\mathcal{S}_2^\infty]$, and multiply them to get a bound on $\exp E(F)[\text{tors}]$.

Step 2: Put $\mathcal{S}_1 = \{\ell \in \mathcal{P} \mid \ell \leq \ell_0\}$. By Theorem 2.8, we have

$$\exp E(F)[\mathcal{S}_1^\infty] \leq C_1(d_0, \ell_0)[F : F_0]^{\frac{1}{2}} \leq C_1(d_0, \ell_0) d^{1/2}.$$

Step 3: Let

$$\mathcal{S}_2 = \{\ell \in \mathcal{P} \mid \ell > \ell_0 \text{ and } b_\ell \geq 1\}.$$

List the elements of $\mathcal{S}_2$ in decreasing order:

$$\ell_1 > \ell_2 > \cdots > \ell_k.$$

Suppose that $\ell \in \mathcal{S}_2$ and $P \in E(F)$ is a point of order ℓ^{b_ℓ}. By Corollaries 1.10 and 1.14, for each prime $\mathfrak{l}$ of F_0 lying above ℓ, there is a positive integer $c \leq 12d_0$ and a prime $\mathcal{L}$ of $F_0(P)$ lying above $\mathfrak{l}$ with $e(\mathcal{L}/\mathfrak{l})$ divisible by either $\varphi(\ell^{b_\ell})/\gcd(\varphi(\ell^{b_\ell}), c)$ or ℓ^{b_ℓ}. Thus, $e(\mathcal{L}/\ell)$ is divisible by either $\varphi(\ell^{b_\ell})/\gcd(\varphi(\ell^{b_\ell}), (12d_0)!)$ or by ℓ^{b_ℓ}.

For simplicity, from now on we write the exponent on ℓ_i as b_i rather than b_{ℓ_i}. Let $P_1, \ldots, P_k$ be F-rational torsion points of orders $\ell_1^{b_1}, \ldots, \ell_k^{b_k}$. Choose $D_1, \ldots, D_k$ with

$$D_i \in \{\varphi(\ell_i^{b_i})/\gcd(\varphi(\ell_i^{b_i}), (12d_0)!), \ell_i^{b_i}\}$$

and such that the field $F_0(P_i)$ has a prime $\mathcal{L}_i$ above ℓ_i with $e(\mathcal{L}_i/\ell_i)$ divisible by D_i.

We introduce the sequence of fields $K_{-1} = F_0$, $K_0 = F_0(E[12])$, $K_1 = K_0(P_1)$, $K_2 = K_1(P_2)$, $\ldots$, $K_k = K_{k-1}(P_k)$. By a result of Raynaud, $E_{/K_0}$ has everywhere semistable reduction; see e.g. [SZ95, Thm. 3.5]. Since $K_k \subset F(E[12])$, we have

$$\prod_{i=0}^{k} [K_i : K_{i-1}] = [K_k : F_0] \leq [F(E[12]) : \mathbb{Q}] = [F(E[12]) : F] \cdot d \leq 4608d. \tag{3.1}$$

(We used here that $\#\,\mathrm{GL}_2(\mathbb{Z}/12\mathbb{Z}) = 4608$.) Moreover,

$$[K_1 : K_0][K_0 : K_{-1}] = [K_1 : F_0] \geq [F_0(P_1) : F_0] = \frac{1}{d_0}[F_0(P_1) : \mathbb{Q}] \geq \frac{D_1}{d_0}. \tag{3.2}$$

Now let us look at $[K_i : K_{i-1}]$ where $i \geq 2$. For notational simplicity, let $\ell = \ell_i$. Since $K_i \supset F_0(P_i)$, we know there is a prime $\mathcal{L}$ of K_i above ℓ for which $e(\mathcal{L}/\ell)$ is divisible by D_i. Define prime ideals $\mathcal{L}_j$ of $\mathbb{Z}_{K_j}$, for $j = -1, 0, 1, \ldots, i$, by

$$\mathcal{L}_j = K_j \cap \mathcal{L}.$$

Thus, $\mathcal{L}_i = \mathcal{L}$, and

$$D_i \mid e(\mathcal{L}/\ell) = e(\mathcal{L}_{-1}/\ell)e(\mathcal{L}_0/\mathcal{L}_{-1}) \prod_{j=1}^{i} e(\mathcal{L}_j/\mathcal{L}_{j-1}).$$

Since $e(\mathcal{L}_{-1}/\ell) \leq d_0$ and $e(\mathcal{L}_0/\mathcal{L}_{-1}) \mid [F_0(E[12]) : F_0] \mid 4608$, it follows that

$$D_i \mid d_0! \cdot 4608 \cdot \prod_{j=1}^{i} e(\mathcal{L}_j/\mathcal{L}_{j-1}). \tag{3.3}$$

Suppose that $1 \leq j < i$. We have

$$K_j = K_{j-1}(P_j) \subset K_{j-1}(E[\ell_j^{b_j}]).$$

Hence, $e(\mathcal{L}_j/\mathcal{L}_{j-1})$ divides the ramification index of $\mathcal{L}_{j-1}$ in $K_{j-1}(E[\ell_j^{b_j}])$. Note that $\mathcal{L}_{j-1}$ lies above the rational prime $\ell = \ell_i$, which is distinct from ℓ_j (since $j < i$). By Lemma 3.1, the ramification index of $\mathcal{L}_{j-1}$ in $K_{j-1}(E[\ell_j])$ divides ℓ_j. Moreover,

$$[K_{j-1}(E[\ell_j^{b_j}]) : K_{j-1}(E[\ell_j])]$$

is a power of ℓ_j. (The image of the representation on the $\ell_j^{b_j}$-torsion lands in the kernel of the natural map $\mathrm{GL}_2(\mathbb{Z}/\ell_j^{b_j}\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/\ell_j\mathbb{Z})$, an ℓ_j-group.) Thus, the ramification index of $\mathcal{L}_{j-1}$ in $K_{j-1}(E[\ell_j^{b_j}])$ is a power of ℓ_j. So $e(\mathcal{L}_j/\mathcal{L}_{j-1})$ is also a power of ℓ_j.

The definition of D_i and the ordering of the primes $\ell_1, \ldots, \ell_k$ imples that D_i is coprime to $\ell_1, \ldots, \ell_{i-1}$. Since $e(\mathcal{L}_j/\mathcal{L}_{j-1})$ is a power of ℓ_j for $j < i$, (3.3) implies that

$$D_i \mid d_0! \cdot 4608 \cdot e(\mathcal{L}/\mathcal{L}_{i-1}), \quad \text{whence} \quad e(\mathcal{L}/\mathcal{L}_{i-1}) \geq \frac{D_i}{4608 \cdot d_0!}.$$

Therefore,

$$[K_i : K_{i-1}] \geq e(\mathcal{L}_i/\mathcal{L}_{i-1}) \geq \frac{D_i}{4608 \cdot d_0!} \qquad (\text{for } 2 \leq i \leq k).$$

From the definition of D_i, it is easy to see that every

$$D_i \geq \frac{\ell_i^{b_i}}{2 \cdot (12d_0)!}.$$

Combining these estimates with (3.1) and (3.2), we find that

$$\begin{aligned} 4608d \geq \prod_{i=0}^{k} [K_i : K_{i-1}] &= [K_0 : K_{-1}][K_1 : K_0] \prod_{2 \leq i \leq k} [K_i : K_{i-1}] \\ &\geq \frac{D_1}{d_0} \cdot \prod_{2 \leq i \leq k} \frac{D_i}{4608 \cdot d_0!} \geq \prod_{i=1}^{k} \frac{\ell_i^{b_i}}{9216 \cdot (12d_0)!^2}. \end{aligned} \tag{3.4}$$

Put

$$Z_0 = 9216 \cdot (12d_0)!^2.$$

Let $Z > Z_0$ be a constant (depending on d_0 and ϵ) to be specified momentarily. If $\ell_i^{b_i} > Z$, then the ith factor in the last displayed product on i is at least $\frac{Z}{Z_0}$. Hence, there can be at most $\log(4608d)/\log(Z/Z_0)$ such values of i. There are at most $\pi(Z)$ values of i with $\ell_i^{b_i} \leq Z$, where $\pi(\cdot)$ is the usual prime-counting function. So

$$k \leq \pi(Z) + \frac{\log(4608d)}{\log(Z/Z_0)}.$$

We may now deduce from (3.4) that

$$\prod_{i=1}^{k} \ell_i^{b_i} \leq Z_0^k \cdot 4608d \leq Z_0^{\pi(Z)} \cdot 4608^{1+\log(Z)/\log(Z/Z_0)} \cdot d^{1+\log(Z_0)/\log(Z/Z_0)}.$$

We fix Z large enough, in terms of d_0 and ϵ, to make $\log(Z_0)/\log(Z/Z_0) < \epsilon$; then

$$\exp E(F)[\mathcal{S}_2^\infty] = \prod_{i=1}^{k} \ell_i^{b_i} \leq C_2(d_0, \epsilon) d^{1+\epsilon}.$$

Step 4: Putting the contribution from $\mathcal{S}_1$ and $\mathcal{S}_2$ together,

$$\exp E(F)[\text{tors}] \leq C_1(d_0, \ell_0) d^{1/2} \cdot C_2(d_0, \epsilon) d^{1+\epsilon} \leq C(d_0, \ell_0, \epsilon) d^{3/2+\epsilon},$$

as desired.

3.3. **From the exponent to the order**

Let $\mathcal{F}$ be a set, each element of which is an elliptic curve defined over a number field $E_{/F}$, and such that for some $B > 0$ and all $E_{/F} \in \mathcal{F}$ we have

$$\exp E(F)[\text{tors}] = O([F : \mathbb{Q}]^B).$$

(The implied constant is allowed to depend on $\mathcal{F}$, but *not* on the choice of $E_{/F} \in \mathcal{F}$.) Let $b = \exp E(F)[\text{tors}]$. Then there is a positive integer a dividing b such that

$$E(F)[\text{tors}] \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}.$$

Since E has full a-torsion over F, the field F contains $\mathbb{Q}(\mu_a)$, so that $[F : \mathbb{Q}] \geq \varphi(a)$. It follows (cf. [HW08, Thms. 327, 328]) that for all $\epsilon > 0$, we have

$$a = O_\epsilon([F : \mathbb{Q}]^{1+\epsilon}).$$

So

$$\#E(F)[\text{tors}] = ab = O_\epsilon([F : \mathbb{Q}]^{B+1+\epsilon}),$$

the implied constant depending on ϵ (and $\mathcal{F}$) but *not* on the choice $E_{/F} \in \mathcal{F}$.

Applying this with $B = \frac{3}{2}$ gives a bound $O_\epsilon([F : \mathbb{Q}]^{\frac{5}{2}+\epsilon})$ on the size of the torsion subgroup, completing the proofs of Theorems 1.5, 1.6 and 1.7.

References

[Ab96] D. Abramovich, *A linear lower bound on the gonality of modular curves*. Internat. Math. Res. Notices 1996, 1005–1011.

[Ar08] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves*. J. Théor. Nombres Bordeaux 20 (2008), 23–43.

[BC16] A. Bourdon and P.L. Clark, *Torsion points and Galois represenations on CM elliptic curves*, `http://arxiv.org/abs/1612.03229`.

[Br10] F. Breuer, *Torsion bounds for elliptic curves and Drinfeld modules*. J. Number Theory 130 (2010), 1241–1250.

[Cl09] P.L. Clark, *On the Hasse principle for Shimura curves*. Israel J. Math. 171 (2009), 349–365.

[CMP17] P.L. Clark, M. Milosevic and P. Pollack, *Typically bounding torsion*, preprint.
[CP15] P.L. Clark and P. Pollack, *The truth about torsion in the CM case.* C.R. Acad. Sci. Paris 353 (2016), 683–688.
[CP17] ———, *The truth about torsion in the CM case, II.* To appear in the Quarterly Journal of Mathematics.
[CT12] A. Cadoret and A. Tamagawa, *A uniform open image theorem for ℓ-adic representations, I.* Duke Math. J. 161 (2012), 2605–2634.
[CT13] ———, *A uniform open image theorem for ℓ-adic representations, II.* Duke Math. J. 162 (2013), 2301–2344.
[De16] M. Derickx, *Torsion points on elliptic curves over number fields of small degree.* Leiden PhD thesis, 2016.
[FJ] M. Fried and M. Jarden, *Field arithmetic.* Third edition. Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, Berlin, 2008.
[Fr94] G. Frey, *Curves with infinitely many points of fixed degree.* Israel J. Math. 85 (1994), 79–83.
[HS99] M. Hindry and J. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique.* C. R. Acad. Sci. Paris 329 (1999), 97–100.
[HW08] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers.* Sixth edition. Oxford University Press, Oxford, 2008.
[La65] M. Lazard, *Groupes analytiques p-adiques.* Inst. Hautes tudes Sci. Publ. Math. No. 26 (1965), 389–603.
[LR15] Á. Lozano-Robledo, *Uniform boundedness in terms of ramification.* `http://alozano.clas.uconn.edu/wp-content/uploads/sites/490/2014/01/lozano-robledo_ramification_bounds_v33.pdf`.
[LV14] E. Larson and D. Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties.* With an appendix by Brian Conrad. J. Inst. Math. Jussieu 13 (2014), 517–559.
[Ma78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld).* Invent. Math. 44 (1978), 129–162.
[Me96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. 124 (1996), 437–449.
[Mo95] F. Momose, *Isogenies of prime degree over number fields.* Compositio Math. 97 (1995), 329–348.
[NS07] N. Nikolov and D. Segal, *On finitely generated profinite groups. I. Strong completeness and uniform bounds.* Ann. of Math. (2) 165 (2007), 171–238.
[Pa99] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres.* J. Reine Angew. Math. 506 (1999), 85–116.
[R-MO] J. Rouse (http://mathoverflow.net/users/48142/jeremy-rouse), *What are the strongest conjectured uniform versions of Serre's Open Image Theorem?*, URL (version: 2015-05-02): `http://mathoverflow.net/q/203837`
[S-LMW] J.-P. Serre, *Lectures on the Mordell-Weil theorem.* Third edition. Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997.
[S-MG] ———, *Abelian ℓ-adic representations and elliptic curves.* Benjamin, New York, 1968.
[Se72] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. 15 (1972), 259–331.
[Si88] A. Silverberg, *Torsion points on abelian varieties of CM-type.* Compositio Math. 68 (1988), 241–249.
[Si92] ———, *Points of finite order on abelian varieties.* In *p-adic methods in number theory and algebraic geometry*, 175–193, Contemp. Math. 133, Amer. Math. Soc., Providence, RI, 1992.
[Si94] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 151, Springer-Verlag, 1994.
[SZ95] A. Silverberg and Yu. G. Zarhin, *Semistable reduction and torsion subgroups of abelian varieties.* Ann. Inst. Fourier (Grenoble) 45 (1995), 403–420.
[Zy15] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, `http://arxiv.org/abs/1508.07660`.