TYPICALLY BOUNDING TORSION

PETE L. CLARK, MARKO MILOSEVIC, AND PAUL POLLACK

Abstract. We formulate the notion of *typical boundedness* of torsion on a family of abelian varieties defined over number fields. This means that the torsion subgroups of elements in the family can be made uniformly bounded by removing from the family all abelian varieties defined over number fields of degree lying in a set of arbitrarily small density. We show that for each fixed g, torsion is typically bounded on the family of all g-dimensional CM abelian varieties. We show that torsion is *not* typically bounded on the family of all elliptic curves, and we establish results – some unconditional and some conditional – on typical boundedness of torsion of elliptic curves for which the degree of the j-invariant is fixed.

1. Introduction

1.1. Notation and terminology

For a subset $\mathcal{S} \subset \mathbb{Z}^+$, we define the *upper density*

$$\overline{\delta}(\mathcal{S}) := \limsup_{x\to\infty} \frac{\#(\mathcal{S} \cap [1,x])}{x}$$

and the *lower density*

$$\underline{\delta}(\mathcal{S}) := \liminf_{x\to\infty} \frac{\#(\mathcal{S} \cap [1,x])}{x}.$$

When $\overline{\delta}(\mathcal{S}) = \underline{\delta}(\mathcal{S})$, we denote it by $\delta(\mathcal{S})$ and call it the *asymptotic density* of $\mathcal{S}$.

For a field F, let F^{sep} be a separable algebraic closure of F and let $\mathfrak{g}_F := \mathrm{Aut}(F^{\mathrm{sep}}/F)$ be the absolute Galois group of F. For an abelian variety $A_{/F}$, we write $\mathrm{End}\, A$ for the endomorphism ring of $A_{/F^{\mathrm{sep}}}$ and $\mathrm{End}^0 A := \mathrm{End}\, A \otimes_{\mathbb{Z}} \mathbb{Q}$, both viewed as $\mathfrak{g}_F$-modules. An abelian variety A has **complex multiplication (CM)** if $\mathrm{End}^0 A$ contains an étale $\mathbb{Q}$-algebra (a finite product of number fields) of degree $2 \dim A$.

1.2. Typical boundedness: a motivating result

Let $T_{\mathrm{CM}}(g,d)$ denote the supremum of $\#A(F)[\mathrm{tors}]$ as F ranges over degree d number fields and A ranges over all CM abelian varieties defined over F. Silverberg [Si88, Si92a] showed that $T_{\mathrm{CM}}(g,d) < \infty$ for all g and d and obtained explicit upper bounds. Sharper results were attained for CM elliptic curves by Silverberg and also recently by several others. Clark-Pollack showed [CP15, CP17a] that

$$\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(1,d)}{d \log\log d} = \frac{e^\gamma \pi}{\sqrt{3}}. \tag{1}$$

Thus the *upper order* of $T_{\mathrm{CM}}(1,d)$ is now known. Work of Bourdon, Clark and Pollack [BCP17] viewed $T_{\mathrm{CM}}(1,d)$ as an "arithmetic function" and studied other aspects of its distribution, in particular giving the following *normal order* result.

Date: March 29, 2018.

Theorem 1.1 ([BCP17, Thm. 1.1a])**.** *For all $\epsilon > 0$, there is $B_\epsilon \in \mathbb{Z}^+$ such that*

$$\overline{\delta}(\{d \in \mathbb{Z}^+ \mid T_{\mathrm{CM}}(1,d) \geq B_\epsilon\}) \leq \epsilon.$$

1.3. **Typical boundedness: definition and first examples**

By a *family of abelian varieties*, we mean a class $\mathcal{F}$ each of whose elements is an abelian variety defined over a number field. (We will only consider classes such that if $(A_1)_{/F}$ lies in $\mathcal{F}$ then any F-isomorphic abelian variety $(A_2)_{/F}$ also lies in $\mathcal{F}$.) Thus for instance we are permitted to take $\mathcal{F}$ to be the family of all abelian varieties over all number fields. We say that *torsion is typically bounded on $\mathcal{F}$* if for all $\epsilon > 0$, there is $B_\epsilon \in \mathbb{Z}^+$ such that the set

$$\mathcal{S}(\mathcal{F}, B_\epsilon) \coloneqq \{d \in \mathbb{Z}^+ \mid \exists\ A_{/F} \in \mathcal{F} \text{ such that } [F:\mathbb{Q}] = d \text{ and } \#A(F)[\mathrm{tors}] \geq B_\epsilon\}$$

has upper density at most ϵ.

Remark 1.2. If $\mathcal{F}_1, \ldots, \mathcal{F}_n$ are families of abelian varieties, then torsion is typically bounded on $\mathcal{F}_i$ for all $1 \leq i \leq n$ iff torsion is typically bounded on $\bigcup_{i=1}^n \mathcal{F}_i$.

We can rephrase Theorem 1.1 as follows:

Theorem 1.3. *Torsion is typically bounded on the family $\mathcal{A}_{\mathrm{CM}}(1)$ of all CM elliptic curves (over all number fields).*

In this paper we study typical boundedness of torsion in several other natural families of abelian varieties. The following example shows that certain kinds of families must be avoided for rather trivial reasons.

Example 1.4. Torsion is *not* typically bounded on the family $\mathcal{A}_{\mathrm{CM}}$ of all CM abelian varieties (over all number fields). Indeed, we have $T_{\mathrm{CM}}(1,1) = 6$ [Ols74], so there is a CM elliptic curve $E_{/\mathbb{Q}}$ with $\#E(\mathbb{Q})[\mathrm{tors}] = 6$. Then for all $g \in \mathbb{Z}^+$, the abelian variety $E^g_{/\mathbb{Q}}$ has CM and $\#E^g(\mathbb{Q})[\mathrm{tors}] = 6^g$. Thus for every number field F we have $\#E^g_{/F}(F)[\mathrm{tors}] \geq 6^g$, so for all $B \in \mathbb{Z}^+$ we have $\mathcal{S}(\mathcal{A}_{\mathrm{CM}}, B) = \mathbb{Z}^+$.

Example 1.4 is not really about complex multiplication. Rather it shows: if a family $\mathcal{F}$ is closed under taking powers of abelian varieties and contains an element with nontrivial torsion subgroup, then torsion is not typically bounded on $\mathcal{F}$.

Example 1.5. (B. Kaydets) For a prime $p > 2$, consider the hyperelliptic curve

$$(C_p)_{/\mathbb{Q}} : y^2 = x^p + 1.$$

Let $O \in C_p(\mathbb{Q})$ be the point at ∞. The Jacobian $(J_p)_{/\mathbb{Q}} \coloneqq \mathrm{Pic}^0(C_p)$ is a geometrically simple CM abelian variety of dimension $\frac{p-1}{2}$ (see e.g. [Sh, p. 113]). Let $\iota\colon C_p(\mathbb{Q}) \hookrightarrow J_p(\mathbb{Q})$ be induced by $P \mapsto [P] - [O]$. Then $\iota((0,1)) \in J_p(\mathbb{Q})$ has order p. Thus torsion is not typically bounded on the family of all geometrically simple abelian varieties.

1.4. **Typical boundedness: main results**

Our first result is a direct generalization of Theorem 1.3.

Theorem 1.6. *For all $g \in \mathbb{Z}^+$, torsion is typically bounded on the family $\mathcal{A}_{CM}(g)$ of all g-dimensional CM abelian varieties (over all number fields).*

The next result was communicated to us by Filip Najman.

Theorem 1.7. *Let $\mathcal{A}(1)$ be the family of all elliptic curves (over all number fields). For each $B \in \mathbb{Z}^+$, the set $\mathcal{S}(\mathcal{A}(1), B)$ contains all but finitely many positive integers. Thus torsion is* not *typically bounded on $\mathcal{A}(1)$.*

So we must restrict the family $\mathcal{A}(1)$ in some way to get typical boundedness. Our remaining results address this.

Theorem 1.8. *Let F_0 be a number field that does not contain the Hilbert class field of any imaginary quadratic field. If $[F_0 : \mathbb{Q}] \geq 3$, we assume the Generalized Riemann Hypothesis (GRH). Then torsion is typically bounded on the family $\mathcal{E}_{F_0}$ of all elliptic curves E defined over a number field $F \supset F_0$ such that $j(E) \in F_0$.*

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

$\mathrm{SI}(d_0)$: There is a 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.

Remark 1.9. When $d_0 = 1$, Mazur showed that $\mathrm{SI}(d_0)$ holds and that the optimal value of ℓ_0 is 37 [Ma78]. Whether $\mathrm{SI}(d_0)$ holds for any $d_0 \geq 2$ is not known, though it is a folk conjecture that $\mathrm{SI}(d_0)$ holds for all $d_0 \in \mathbb{Z}^+$.

Theorem 1.10. *Let $d_0 \in \mathbb{Z}^+$. If $\mathrm{SI}(d_0)$ holds, then torsion is typically bounded on the family $\mathcal{E}_{d_0}$ of all elliptic curves $E_{/F}$ defined over a number field F such that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$.*

Remark 1.11. This paper is cognate to another work [CP17b], written in parallel, giving upper bounds on $\#E(F)[\mathrm{tors}]$ for an elliptic curve E/F that are polynomial in $[F : \mathbb{Q}]$, under the same hypotheses as Theorems 1.8 and 1.10.

1.5. **The plan of the paper**

In §2 we deduce Theorem 1.7 from some general results on degrees of closed points of varieties over Hilbertian fields. Our main tool is the Riemann-Roch theorem.

In §3 we present a formalism for proving typical boundedness of families of abelian varieties, reducing the task to showing divisibilities on the degrees of the field of definition of a torsion point of order a large power of a fixed prime – Condition (P1) – and of the field of definition of a prime order torsion point – Condition (P2). We show a relationship between strong uniform boundedness results and Condition (P1), reducing the proofs of Theorems 1.6, 1.8 and 1.10 to verifying Condition (P2).

In §4 we verify Condition (P2) for $\mathcal{A}_{\mathrm{CM}}(g)$. We use a recent result of Gaudron-Rémond [GR17] that builds on important work of Silverberg [Si88, Si92a].

In §5 we verify Condition (P2) for the families $\mathcal{E}_{F_0}$ and $\mathcal{E}_{d_0}$ under the assumptions in Theorems 1.8 and 1.10, thus proving those results. Our general strategy is heavily influenced by work of Lozano-Robledo [LR13] that gives lower bounds on the degree of the field of definition of a point of prime order p for an elliptic curve defined over $\mathbb{Q}$. Whereas Lozano-Robledo used the complete classification of rational isogenies on elliptic curves over $\mathbb{Q}$, we instead use finiteness theorems of Mazur, Momose and Larson-Vaintrob.

Acknowledgments. Our proof of Theorem 1.6 draws from results in the literature that were brought to our attention by Abbey Bourdon. As mentioned above, Theorem 1.7 was communicated to us by Filip Najman. This result has become a key part of the narrative of our paper, and we are very grateful to him. Theorem 1.10 is part of the thesis work of the second author under the direction of the first author. We

thank Boris Kaydets for contributing Example 1.5 in response to an earlier draft of our paper in which we described the typical boundedness of torsion on the family of all geometrically simple abelian varieties as an open problem.

2. The degrees of closed points on an algebraic variety

In this section we prove Theorem 1.7. As observed by Najman, the key observation is that a curve defined over a number field k that has a k-rational point must have infinitely many closed points of degree d for all sufficiently large d, applied to the modular curves $X_1(N)_{/\mathbb{Q}}$. In fact we will prove a generalization of Najman's observation to closed points on varieties over any Hilbertian field of characteristic zero: Theorem 2.4.

Let k be a field. A **variety** $V_{/k}$ is a finite-type k-scheme. By a **nice variety** $V_{/k}$ we mean a variety that is smooth, projective and geometrically integral.

The natural context of the results of this section is the class of *Hilbertian fields* (see e.g. [FJ]), namely those for which the conclusion of Hilbert's irreducibility theorem holds. For our purposes here it suffices to know that number fields are Hilbertian [FJ, Ch. 13]: Hilbert's theorem.

2.1. Curves with a k-rational point

Theorem 2.1. *Let k be a Hilbertian field of characteristic zero, and let $C_{/k}$ be a nice curve of genus g with at least one k-rational point. Then there is $D \in \mathbb{Z}^+$ such that if $d \geq D$, the curve C has infinitely many closed points of degree d. More precisely:*

a) *If $g = 0$, we may take $D = 1$.*
b) *If $g \geq 1$, we may take $D = 2g$.*
c) *If C has a k-rational point that is not a Weierstrass point, we may take $D = g + 1$.*

Proof. Step 0: If $g = 0$, then since $C(k) \neq \varnothing$ we have $C \cong \mathbb{P}^1$ and thus C has infinitely many closed points of degree d for all $d \in \mathbb{Z}^+$. Henceforth we suppose $g \geq 1$.

Step 1: Let $P \in C(k)$, let K be a canonical divisor for C, and let $d \geq 2g - 1$. Then $\deg(K - d[P]) < 0$, so the Riemann-Roch space $H^0(\mathcal{L}(n[P]))$ has dimension $d - g + 1$. Thus $H^0(\mathcal{L}((d+1)[P])) \supsetneq H^0(\mathcal{L}((d)[P]))$, so for all $d \geq 2g$ there is $f \in k(C)$ with polar divisor $d[P]$, so $f\colon C \to \mathbb{P}^1$ is a morphism of degree d. If P is not a Weierstrass point then $\dim H^0(\mathcal{L}(d[P])) = 1$ for all $1 \leq d \leq g$, and thus $\dim H^0(\mathcal{L}(d[P])) = d + 1 - g$ for all $d \geq g$. As above, there is a degree d morphism $f\colon C \to \mathbb{P}^1$ for all $d \geq g + 1$.

Step 2: Let $f\colon C \to \mathbb{P}^1$ be a morphism of degree d. Since k has characteristic 0, the field extension $k(C)/k(\mathbb{P}^1)$ is separable; let m its Galois closure. Because k is Hilbertian, there are infinitely many $Q \in \mathbb{P}^1(k)$ that are inert in $m/k(\mathbb{P}^1)$, hence also inert in $k(C)/k(\mathbb{P}^1)$. In other words, for infinitely many Q, the fiber $f^*(P)$ of f is a degree d closed point on C. □

Corollary 2.2. *Let $N \in \mathbb{Z}^+$. Then for all $d \geq \max\{1, 2g(X_1(N))\}$, there is a sequence $\{(F_n, E_n, P_n)\}_{n=1}^{\infty}$ such that F_n is a number field of degree d, $(E_n)_{/F_n}$ is an elliptic curve, $j(E_n) \neq j(E_m)$ for all $m \neq n$, $P_n \in E_n(F_n)$ is a point of order N and (E_n, P_n) cannot be defined over any proper subfield of F_n.*

Proof. Let $d \geq \max\{1, 2g(X_1(N))\}$. We apply Theorem 2.1 with $k = \mathbb{Q}$, $C = X_1(N)$ and P the cusp at infinity to get a sequence $\{x_n\}_{n=1}^{\infty}$ of distinct degree d closed points on $X_1(N)$. Since $X_1(N) \to X(1)$ is a finite map, by passing to a subsequence we may assume that $x_n \in Y_1(N)$ for all n and that $j(x_n) \neq j(x_m)$ for all $m \neq n$. Let F_n be the residue field of x_n. Since $Y_1(N)$ is a fine moduli space for $N \geq 4$, each x_n corresponds to a unique pair (E_n, P_n). When $N \leq 3$ we use that the obstruction to being defined over the field of moduli vanishes for closed points on modular curves. Since F_n is the field of moduli of (E_n, P_n), the pair cannot be defined over a proper subfield of F_n. □

Remark 2.3. We have (see e.g. [KK96, Thm. 1]) that

$$g(X_1(N)) = \begin{cases} 0 & \text{if } 1 \leq N \leq 4, \\ 1 + \frac{N^2}{24} \prod_{p|N} \left(1 - \frac{1}{p^2}\right) - \frac{1}{4} \sum_{d|N} \varphi(d)\varphi(\frac{N}{d}) & \text{if } N \geq 5. \end{cases}$$

Thus for all $N \in \mathbb{Z}^+$, we have $g(X_1(N)) \leq N^2/24 + 1$, so Corollary 2.2 implies that for every degree $d \geq N^2/12 + 2$, there is an elliptic curve E over a degree d number field F for which $N \mid \exp E(F)[\text{tors}]$. Moreover, E can be taken to not have CM. Indeed, our examples $E_{/F}$ have infinitely many distinct j-invariants, whereas there are only finitely many CM j-invariants of any given degree. Consequently, defining $T_{\neg \text{CM}}(d)$ as the supremum of $\#E(F)[\text{tors}]$ for a non-CM elliptic curve E defined over a degree d number field F, we have

$$\liminf_d \frac{T_{\neg \text{CM}}(d)}{\sqrt{d}} > 0.$$

On the other hand, by [CP17a, Thm. 6.4] we have

$$\limsup_d \frac{T_{\neg \text{CM}}(d)}{\sqrt{d \log \log d}} \geq \sqrt{\frac{\pi^2 e^{\gamma}}{3}}.$$

Hindry-Silverman [HS99] raised the key open question: is $\limsup_d \frac{T_{\neg \text{CM}}(d)}{\sqrt{d \log \log d}} < \infty$? If yes, then $T_{\neg \text{CM}}(d)$ grows remarkably regularly, in sharp contrast with the CM case (compare eq. (1) with Theorem 1.1).

2.2. **The proof of Theorem 1.7**

Let $\mathcal{A}(1)$ be the family of all elliptic curves (over all number fields). Corollary 2.2 gives: for all $B \in \mathbb{Z}^+$, $\mathcal{S}(\mathcal{A}(1), B)$ contains all but finitely many elements of $\mathbb{Z}^+$, hence has density 1.

2.3. **Arbitrary varieties**

In the setting of Theorem 2.1, without the assumption that $C(k) \neq \varnothing$, the conclusion of Theorem 2.1 need not hold: e.g., if $C_{/k}$ is a nice curve of genus zero with $C(k) = \varnothing$, then (by Riemann-Roch) C has no closed points of any odd degree.

To go further, recall that the **index** $I(V)$ of a nice variety $V_{/k}$ is the least positive degree of a k-rational zero-cycle on V – equivalently, the greatest common divisor of all degrees of closed points on V. Here is an analogue of Theorem 2.1 in the absence of the assumption $C(k) \neq \varnothing$, generalized from curves to all varieties.

Theorem 2.4. *Let k be a Hilbertian field of characteristic zero, and let $V_{/k}$ be a nice variety of positive dimension and index I. There is $D \in \mathbb{Z}^+$ such that for all $d \geq D$, the variety V has infinitely many closed points of degree dI.*

Proof. Step 1: Suppose $C_{/k}$ is a nice curve of genus g. The case $g = 0$ has already been treated above, so suppose $g \geq 1$. Let $P_1, \ldots, P_r$ be distinct closed points of C of degrees $d_1, \ldots, d_r$ such that $\gcd(d_1, \ldots, d_r) = I$. There is a positive integer M such that if an integer d is at least M and divisible by I, then there are $n_1, \ldots, n_r \in \mathbb{N}$ such that $d = n_1 d_1 + \ldots + n_r d_r$: see e.g. [RA, Thm. 1.0.1]. Let

$$D = \max\{M, 2g - 1 + \sum_{i=1}^{r} d_i\}.$$

Let d be an integer such that $d \geq M$ and $I \mid d$, so we may write $d = \sum_{i=1}^r n_i d_i$ for $n_i \in \mathbb{N}$, and we may assume without loss of generality that $n_1 \geq 1$. The divisor $(n_1 - 1)[P_1] + \sum_{i=2}^r n_i[P_i]$ has degree at least $2g - 1$, so by Riemann-Roch we have

$$\dim H^0\mathcal{L}\left(\sum_{i=1}^{r} n_i[P_i]\right) = d_1 + \dim H^0\mathcal{L}\left((n_1 - 1)[P_1] + \sum_{i=2}^{r} n_i[P_i]\right),$$

so there is a rational function on C with polar divisor $\sum_{i=1}^r n_i[P_i]$ and thus a morphism $f\colon C \to \mathbb{P}^1$ of degree d. Step 2 of the proof of Theorem 2.1 again applies to show that C admits infinitely many closed points of degree d.

Step 2: Let $V_{/k}$ be a nice variety of index I. There are closed points $P_1, \ldots, P_r$ of V such that $I = \gcd(\deg(P_1), \ldots, \deg(P_r))$; let Z be the zero-cycle $\sum_{i=1}^r [P_i]$. Then there is a nice curve $C_{/k}$ with $Z \subset C \subset V$: since k is infinite, one may apply an extension of the Bertini Theorem due to Kleiman-Altman [KA79, Thm. (1)]. It follows that C has index I, and applying Step 1 to C finishes the proof. □

Since by definition a variety can only have a closed point of degree d if d is a multiple of the index, Theorem 2.4 determines the set of degrees of closed points on any nice variety over a characteristic zero Hilbertian field *up to a finite set*.

Remark 2.5. Let k be any field, let $C_{/k}$ be a nice curve, and let $f\colon C \to \mathbb{P}^1$ be a morphism of degree d. Pulling back a k-rational point on $\mathbb{P}^1$ yields an effective divisor of degree d and thus $I(C) \mid d$. The **gonality** $\mathrm{gon}(C)$ of C is the least degree of a finite morphism $C \to \mathbb{P}^1$, so we have

$$I(C) \mid \mathrm{gon}(C).$$

We call a curve **I-gonal** if $I(C) = \mathrm{gon}(C)$. Above we saw every genus zero curve is I-gonal and the degrees of closed points on a genus zero curve are precisely the positive integer multiples of $I(C)$. The same argument holds for all I-gonal curves. In some sense, "most curves over most fields" are I-gonal: if $g \geq 2$, $(\mathcal{M}_g)_{/\mathbb{Q}}$ is the moduli scheme of genus g curves, $k = \mathbb{Q}(\mathcal{M}_g)$ is its function field and $C_{/k}$ is a nice curve of genus g with field of moduli k, then $I(C) = \mathrm{gon}(C) = 2g - 2$.

Remark 2.6.

a) Let $\mathbb{F}_q$ be a finite field, and let $C_{/\mathbb{F}_q}$ be a nice curve. The Riemann Hypothesis for C gives $C(\mathbb{F}_{q^d}) \neq \varnothing$ for all sufficiently large d. In particular C has index 1, a result of F.K. Schmidt. If $V_{/\mathbb{F}_q}$ is a nice variety of positive dimension, then by Poonen's finite field Bertini Theorem [Po04], V contains a nice curve $C_{/\mathbb{F}_q}$. So $V_{/\mathbb{F}_q}$ admits at least one closed point of degree d for all sufficiently large d.

b) Some hypothesis on k is necessary to force a nice variety $V_{/k}$ to have closed points of degree $dI(V)$ for all large d: e.g. k must have extensions of these degrees!

3. A criterion for typical boundedness

If r and s are nonzero rational numbers, we write $r \mid s$ if $\frac{s}{r} \in \mathbb{Z}$.

3.1. **Conditions (P1) and (P2)**

Consider the following conditions on a family $\mathcal{F}$ of abelian varieties:

Condition (P1): for all primes p and all $N \in \mathbb{Z}^+$, there is $n = n(p, N, \mathcal{F}) \in \mathbb{Z}^+$ such that for all $A_{/F} \in \mathcal{F}$, if $A(F)$ has a point of order p^n then $p^N \mid [F : \mathbb{Q}]$.

Condition (P2): there is $c = c(\mathcal{F}) \in \mathbb{Z}^+$ such that for all prime numbers p and all $A_{/F} \in \mathcal{F}$, if $A(F)$ has a point of order p then

$$\frac{p-1}{c} \mid [F : \mathbb{Q}].$$

Remark 3.1. For any finite set $\{p_1, \ldots, p_n\}$ of prime numbers, by taking c to be divisible by $\prod_{i=1}^{n}(p_i - 1)$ we get Condition (P2) for these primes automatically. Thus Condition (P2) holds if there is a positive integer $\tilde{c}$ and a number P such that for all primes $p \geq P$ and all $A_{/F} \in \mathcal{F}$, if $A(F)$ has a point of order P then $p - 1 \mid \tilde{c}[F : \mathbb{Q}]$.

Theorem 3.2. *Let $\mathcal{F}$ be a family of abelian varieties over number fields. Suppose $\mathcal{F}$ satisfies Conditions (P1) and (P2). Then:*

a) *The exponent of the torsion subgroup is typically bounded in $\mathcal{F}$. That is, for each $\epsilon > 0$, there is $B_\epsilon \in \mathbb{Z}^+$ such that the set*

$$\{d \in \mathbb{Z}^+ \mid \exists\ A_{/F} \in \mathcal{F} \text{ such that } [F : \mathbb{Q}] = d \text{ and } \exp A(F)[\mathrm{tors}] \geq B_\epsilon\}$$

has upper density at most ϵ.

b) *For $g \in \mathbb{Z}^+$, let $\mathcal{F}_g$ be the elements of $\mathcal{F}$ of dimension g. Then the torsion subgroup is typically bounded in $\mathcal{F}_g$.*

Proof. a) We will use the Erdős-Wagstaff Theorem [EW80, Thm. 2]: for all $\epsilon > 0$, there is C_ϵ such that the set of positive integers admitting a divisor of the form $\ell - 1 > C_\epsilon$ for a prime number ℓ has upper density at most ϵ. It follows easily that for any fixed $c \in \mathbb{Z}^+$, there is $C = C(\epsilon, c)$ such that the set of positive integers d for which there exists a prime $\ell > C$ such that $\frac{\ell-1}{c} \mid d$ has upper density at most ϵ. By Condition (P2), there is $c \in \mathbb{Z}^+$ such that for all $d \in \mathbb{Z}^+$, if $F/\mathbb{Q}$ is a number field of degree d and $A_{/F} \in \mathcal{F}$ with $\ell \mid \#A(F)[\mathrm{tors}]$, we have

$$\frac{\ell - 1}{c} \mid d.$$

Thus, after removing a set of degrees d of upper density at most $\epsilon/2$, we get $L \in \mathbb{Z}^+$ such that if $\ell \mid \#A(F)[\mathrm{tors}]$ for some $A_{/F} \in \mathcal{F}$ with $[F : \mathbb{Q}] = d$, then $\ell \leq L$. For each $\ell \leq L$ and $N \in \mathbb{Z}^+$, the set of d which are divisible by ℓ^N has density ℓ^{-N}, so if N is sufficiently large then the set of positive integers d that are divisible by ℓ^N for some $\ell \leq L$ has density at most $\frac{\epsilon}{2}$. By Condition (P1), there is a positive integer n such that if $\ell \leq L$ and $A_{/F} \in \mathcal{F}$ has a point of order ℓ^{n+1} then $\ell^N \mid [F : \mathbb{Q}]$. This gives a set $\mathcal{D}_\epsilon \subset \mathbb{Z}^+$ of upper density at most ϵ such that if $A_{/F} \in \mathcal{F}$ and $[F : \mathbb{Q}] \notin \mathcal{D}_\epsilon$, then the order of any torsion point on $A(F)$ divides $\prod_{\ell \leq L} \ell^n$. So we may take $B_\epsilon = 1 + \prod_{\ell \leq L} \ell^n$.

b) If $A_{/F}$ is an abelian variety defined over a number field, then

$$\#A(F)[\mathrm{tors}] \mid (\exp A(F)[\mathrm{tors}])^{2 \dim A}.$$

The result follows immediately from this and from part a). □

3.2. **Merelian families**

We say that a family $\mathcal{F}$ of abelian varieties is *Merelian* if for all $d \in \mathbb{Z}^+$, there is $B = B(d, \mathcal{F}) \in \mathbb{Z}^+$ such that for all degree d number fields F, if $A_{/F} \in \mathcal{F}$ then $\#A(F)[\mathrm{tors}] \leq B(d)$.

Example 3.3.

a) (Merel [Me96]) The family $\mathcal{E} = \mathcal{A}(1)$ of all elliptic curves is Merelian.
b) It is believed that for all $g \geq 2$ the family $\mathcal{A}(g)$ of all g-dimensional abelian varieties is Merelian, but this seems to lie far out of reach.
c) (Silverberg [Si88]) Fix $g \geq 1$. The family $\mathcal{A}_{\mathrm{CM},g}$ of g-dimensional abelian varieties with complex multiplication is Merelian.
d) Work of Clark-Xarles [CX08] produces Merelian families $\mathcal{F}_g$ with

$$\mathcal{A}_{\mathrm{CM},g} \subsetneq \mathcal{F}_g \subsetneq \mathcal{A}_g.$$

For instance, one can take for $\mathcal{F}_g$ the family of all g-dimensional $A_{/F}$ such that F admits a place $v_2 \mid 2$ and a place $v_3 \mid 3$ such that at each of the two places the Néron special fiber contains no copy of the multiplicative group $\mathbb{G}_m$. (This family contains in particular all $A_{/F} \in \mathcal{A}_g$ with algebraic integral moduli and thus $\mathcal{F}_g \setminus \mathcal{A}_{\mathrm{CM},g}$ is infinite.)

Theorem 3.4. *Let $\mathcal{F}$ be a family of abelian varieties over number fields that is closed under base extension, and let $\mathcal{F}_{g,d}$ be the subfamily of $\mathcal{F}_g$ consisting of all g-dimensional abelian varieties $A_{/F}$ such that there is a subfield $F_0 \subset F$ with $[F_0 : \mathbb{Q}] = d$ and an abelian variety $(A_0)_{/F_0}$ such that $(A_0)_{/F} \cong A_{/F}$. If $\mathcal{F}_{g,d}$ is Merelian, then it satisfies Condition (P1).*

Proof. Fix a prime number p and a positive integer N. If $A_{/F} \in \mathcal{F}_{g,d}$, then $\dim A = g$ and there is a subfield $F' \subset F$ with $[F' : \mathbb{Q}] = d$ such that A has a model over F'. Let $P \in A(F)$ have order p^n for some $n \geq N$. Then $F'(P) \subset F'(A[p^n])$, so

$$[F'(P) : F'] \mid [F'(A[p^n]) : F'] \mid \#\,\mathrm{GL}_{2g}(\mathbb{Z}/p^n\mathbb{Z}).$$

Since

$$\#\,\mathrm{GL}_{2g}(\mathbb{Z}/p\mathbb{Z}) = \prod_{i=0}^{2g-1} \left(p^{2g} - p^i\right)$$

and

$$\#\,\mathrm{GL}_{2g}(\mathbb{Z}/p^{n+1}\mathbb{Z}) = p^{4g^2} \#\,\mathrm{GL}_{2g}(\mathbb{Z}/p^n\mathbb{Z}),$$

there is a positive integer c with $\gcd(c, p) = 1$ that depends on p and g but not on n and a positive integer G (depending on g and n but not on p) such that

$$\#\,\mathrm{GL}_{2g}(\mathbb{Z}/p^n\mathbb{Z}) = cp^G.$$

Because $\mathcal{F}_{g,d}$ is Merelian, if n is sufficiently large compared to N then

$$[F'(P) : F'] \geq cp^N.$$

It follows that

$$p^N \mid [F'(P) : F'] \mid [F : \mathbb{Q}]. \qquad \square$$

Theorem 3.5. *Let $d_0 \in \mathbb{Z}^+$. The family $\mathcal{E}_{d_0}$ of all elliptic curves $E_{/F}$ defined over number fields such that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$ satisfies Condition (P1).*

Proof. Combining Theorem 3.4 with Merel's Theorem shows: the family of elliptic curves arising by base extension from a number field of degree d_0 satisfies Condition (P1). Fix p a prime number, N a positive integer, and let $n \in \mathbb{Z}^+$ be such that for every elliptic curve $E_{/F}$ arising by base extension from a number field of degree d_0 such that $E(F)$ has a point of order p^n, we have $p^{N+2} \mid [F : \mathbb{Q}]$.

Let F be any number field, let $E_{/F}$ be an elliptic curve with $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$, and suppose that $E(F)$ has a point of order p^n. Let $F_0 = \mathbb{Q}(j(E))$, let $(E_0)_{/F_0}$ be any elliptic curve. Then $F_0 \subset F$, and there is F'/F of degree dividing 12 such that $E_{/F'} \cong (E_0)_{/F'}$. Then $E_0(F') \cong E(F') \supset E(F)$ has a point of order p^n, so

$$p^{N+2} \mid [F' : \mathbb{Q}] = [F' : F][F : \mathbb{Q}] \mid 12[F : \mathbb{Q}],$$

and thus

$$\mathrm{ord}_p[F : \mathbb{Q}] \geq N. \qquad \square$$

4. The proofs of Theorems 1.6, 1.8 and 1.10

4.1. The proof of Theorem 1.6

Theorem 4.1 (Gaudron-Rémond [GR17])**.** *Let $A_{/F}$ be an abelian variety defined over a number field. Suppose A has complex multiplication and $\mathrm{End}_F A = \mathrm{End}\, A$. Let μ be the number of roots of unity in the center of $\mathrm{End}\, A$. Let e be the exponent of $A(F)[\mathrm{tors}]$. Then*

$$\varphi(e) \mid \frac{\mu}{2}[F : \mathbb{Q}]. \tag{2}$$

Corollary 4.2. *Let $g \in \mathbb{Z}^+$. There is a positive integer $c(g)$ such that: for all number fields F and all g-dimensional CM abelian varieties $A_{/F}$, if $A(F)$ has a point of order N, then*

$$\varphi(N) \mid c(g)[F : \mathbb{Q}].$$

Proof. Step 1: There is $H(g) \in \mathbb{Z}^+$ such that for every g-dimensional abelian variety A defined over a field F of characteristic zero, there is a field extension K/F with $[K : F] \mid H(g)$ such that $\mathrm{End}_K A_{/K} = \mathrm{End}\, A$. This can be proved by observing that $\mathrm{End}\, A \cong \mathbb{Z}^d$ for some $1 \leq d \leq 2g^2$ and thus the action of $\mathfrak{g}_F$ on $\mathrm{End}\, A$ is given by a homomorphism $\mathfrak{g}_F \to \mathrm{GL}_d(\mathbb{Z})$ with finite image, and using a result of Minkowski [Mi87] (see also the work of Friedland [Fr97]) that there is an absolute bound on the size of a finite subgroup of $\mathrm{GL}_d(\mathbb{Z})$.[1] We get a variant of Theorem 4.1 in which the hypothesis $\mathrm{End}_F A = \mathrm{End}\, A$ is dropped and the conclusion is $\varphi(e) \mid \frac{H(g)\mu}{2}[F : \mathbb{Q}]$.

Step 2: We claim that there is $M(g) \in \mathbb{Z}^+$ such that if $A_{/F}$ is a g-dimensional CM abelian variety with $\mathrm{End}_F A = \mathrm{End}\, A$ then the number of roots of unity in the center of $\mathrm{End}\, A$ divides $M(g)$. Let Z be the center of $\mathrm{End}\, A$ and Z^0 be the center of $\mathrm{End}^0 A$. Then Z^0 is an étale $\mathbb{Q}$-algebra of dimension $2g$ [Mi, Prop. 1.3 and §3], i.e., there are number fields $F_1, \ldots, F_r$ such that $Z^0 \cong \prod_{i=1}^r F_i$ and $2g = \dim Z^0 = \prod_{i=1}^r [F_i : \mathbb{Q}]$. Thus Z is isomorphic to a subring of $\prod_{i=1}^r \mathbb{Z}_{F_i}$, where $\mathbb{Z}_{F_i}$ is the ring of integers of F_i, so if μ_i is the number of roots of unity in F_i then $\mu \mid \prod_{i=1}^r \mu_i$. The number of roots of unity in a number field F is bounded in terms of $[F : \mathbb{Q}]$ – indeed, if this number is

[1] This does not lead to a very good bound. Better bounds occur as a special case of work of Silverberg [Si92b]. Recent work of Guralnick-Kedlaya [GK16] computes the optimal value of $H(g)$ for all g, and recent work of Rémond [Re17] computes the maximal value of $[K : F]$ for each g.

N, then $F \subset \mathbb{Q}(\zeta_N)$, so $\varphi(N) \mid [F : \mathbb{Q}]$ and $N = O([F : \mathbb{Q}] \log\log[F : \mathbb{Q}])$. Moreover $r \leq 2g$ and $[F_i : \mathbb{Q}] \leq 2g$ for all i. This establishes the claim, and the result follows. □

Let p be a prime number, let $N \in \mathbb{Z}^+$, and let $A_{/F}$ be a g-dimensional CM abelian variety defined over a number field. Using Corollary 4.2, we get:

- If $N \in \mathbb{Z}^+$, if $A(F)$ has a point of order $p^{N+\mathrm{ord}_p(c(g))+1}$ then
$$\varphi(p^{N+\mathrm{ord}_p(c(g))+1}) = (p-1)p^{N+\mathrm{ord}_p(c(g))} \mid c(g)[F : \mathbb{Q}],$$
so $p^N \mid [F : \mathbb{Q}]$. So Condition (P1) holds for the family $\mathcal{A}_{\mathrm{CM}}(g)$.
- If $A(F)$ has a point of order p then $p - 1 = \varphi(p) \mid c(g)[F : \mathbb{Q}]$, establishing Condition (P2) for the family $\mathcal{A}_{\mathrm{CM}}(g)$.

By Theorem 3.2, torsion is typically bounded on $\mathcal{A}_{\mathrm{CM}}(g)$.

4.2. **The proofs of Theorems 1.8 and 1.10**

Theorem 3.5 reduces the proofs of Theorems 1.8 and 1.10 to the following result.

Theorem 4.3.

a) *Let $d_0 \in \mathbb{Z}^+$ be such that* SI(d_0) *holds. The family $\mathcal{E}_{d_0}$ of all elliptic curves defined over number fields such that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$ satisfies condition (P2).*

b) *Let F_0 be a number field that does not contain the Hilbert class field of any imaginary quadratic field. If $[F_0 : \mathbb{Q}] \geq 3$ then we assume the Generalized Riemann Hypothesis (GRH). Then the family $\mathcal{E}_{F_0}$ of all elliptic curves defined over a number field $F \supset F_0$ such that $j(E) \in F_0$ satisfies condition (P2).*

We begin the proof of Theorem 4.3. In view of the work of [BCP17] (or Theorem 1.6) we may restrict attention to elliptic curves *without* CM. We will prove part a) and then discuss the (minor) modifications necessary to prove part b).

Let $d_0 \in \mathbb{Z}^+$ be such that SI(d_0) holds. For $E_{/F} \in \mathcal{E}_{d_0}$, let $F_0 = \mathbb{Q}(j(E))$ and let $(E_0)_{/F_0}$ be an elliptic curve with $j(E_0) = j(E)$, so $F_0 \subset F$. Since E has no CM, there is a quadratic extension F'/F such that $E_{/F'} \cong (E_0)_{/F'}$ (see e.g. [Si86, §X.5]). Since $[F' : \mathbb{Q}] = 2[F : \mathbb{Q}]$, if the family $\mathcal{G}_{d_0}$ of all elliptic curves $E_{/F}$ that arise by base extension from $(E_0)_{/\mathbb{Q}(j(E_0))}$ with $[\mathbb{Q}(j(E_0)) : \mathbb{Q}] = d_0$ satisfies condition (P2) for some $c \in \mathbb{Z}^+$, then the family $\mathcal{E}_{d_0}$ satisfies (P2) for $2c$. So we may work with $\mathcal{G}_{d_0}$.

Let F_0 be a number field of degree d_0, and let $(E_0)_{/F_0}$ be an elliptic curve with $\mathbb{Q}(j(E)) = F_0$. Let p be a prime number, let
$$\rho_p \colon \mathfrak{g}_{F_0} \to \mathrm{GL}(E_0[p])$$
be the mod p Galois representation attached to $(E_0)_{/F_0}$, let $G = \rho_p(\mathfrak{g}_{F_0})$ be its image, and let $\overline{G}$ be its projective image, i.e., the image of G under the homomorphism $\mathrm{GL}(E_0[p]) \to \mathrm{PGL}(E_0[p])$. The degrees of extensions F/F_0 such that $E_0(F)$ has a point of order p are the multiples of the sizes of the orbits of G on $E_0[p] \setminus \{0\}$. Thus it is enough to show that there is $c = c(d_0)$ such that for all $(E_0)_{/F_0}$ as above and for all nonzero $P \in E_0[p]$, we have
$$\frac{p-1}{c} \,\Big|\, [F_0(P) : \mathbb{Q}].$$
Recall that $\det \rho_p \colon \mathfrak{g}_{F_0} \to (\mathbb{Z}/p\mathbb{Z})^\times$ is the mod p cyclotomic character χ_p. Let
$$i(p) = [(\mathbb{Z}/p\mathbb{Z})^\times : \chi_p(\mathfrak{g}_{F_0})].$$

Then $i(p)$ depends on F_0 and not just d_0, but harmlessly: since $\chi_p(\mathfrak{g}_{\mathbb{Q}}) = (\mathbb{Z}/p\mathbb{Z})^\times$, we have $i(p) \mid d_0$. In particular, we have in all cases that

$$\frac{p-1}{d_0} \,\Big|\, \frac{p-1}{i(p)} \,\Big|\, \#G.$$

A choice of $\mathbb{F}_p$-basis e_1, e_2 for $E_0[p]$ induces an isomorphism $\mathrm{GL}(E_0[p]) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{F}_p)$, thus G may be viewed as a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, well-defined up to conjugacy. We recall the classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ – essentially due to Dickson, and given in [Se72, §2.4, §2.6]: for $G \subset \mathrm{GL}_2(\mathbb{F}_p)$, at least one of the following holds:

(1) The subgroup G contains $\mathrm{SL}(E_0[p])$.
(2) The subgroup G is contained in the normalizer of a split Cartan.
(3) The subgroup G is contained in the normalizer of a nonsplit Cartan.
(4) The subgroup $\overline{G}$ is isomorphic to A_4, S_4 or A_5.
(5) The subgroup G is contained in a Borel.

We will address each of these cases separately.

4.2.1. *Case 1.* Suppose $G = \rho_p(\mathfrak{g}_{F_0})$ contains $\mathrm{SL}_2(E_0[p])$. Then

$$[\mathrm{GL}_2(E_0[p]) : G] \mid i(p) \mid d_0.$$

Since $\mathrm{GL}(E_0[p])$ acts transitively on $E_0[p] \setminus \{0\}$, the size of any orbit of G on $E_0[p] \setminus \{0\}$ is divisible by

$$\frac{\#(E_0[p] \setminus \{0\})}{d_0} = \frac{(p+1)(p-1)}{d_0}.$$

Thus $\frac{p-1}{d_0} \mid [F_0(P) : F_0]$, so $p - 1 \mid [F_0(P) : \mathbb{Q}]$: we may take $c = 1$.

4.2.2. *Case 2.* A split Cartan subgroup C_s of $\mathrm{GL}_2(E_0[p])$ is the set of matrices $m \in \mathrm{GL}_2(\mathbb{F}_p)$ that pointwise fix each of a pair L_1, L_2 of one-dimensional subspaces of $E_0[p]$. Its normalizer NC_s is the set of matrices $m \in \mathrm{GL}_2(\mathbb{F}_p)$ that stabilize the pair $\{L_1, L_2\}$, i.e., either $mL_1 = L_1$ and $mL_2 = L_2$ (so $m \in C_s$) or $mL_1 = L_2$ and $mL_2 = L_1$ (so $m \notin C_s$). Choosing a basis such that e_1 generates L_1 and e_2 generates L_2, these groups are given explicitly as

$$C_s = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \,\middle|\, a, b \in \mathbb{F}_p^\times \right\},$$

$$NC_s = C_s \coprod \left\{ \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} \,\middle|\, c, d \in \mathbb{F}_p^\times \right\}.$$

In particular, if G is contained in a split Cartan, then it is contained in a Borel subgroup, namely the set of matrices $m \in \mathrm{GL}_2(E_0[p])$ that fix a single line L. This is taken care of in Case 5 below. So suppose that G is contained in NC_s but not contained in C_s. Let $F \supset F_0$ be a number field such that $E_0(F)$ has a point P of order p. Then $\rho_p|_{\mathfrak{g}_F}$ has image contained in NC_s and also fixes P and thus the one-dimensional subspace $L = \langle P \rangle$, so the following result applies with $H = \rho_p(\mathfrak{g}_F)$.

Lemma 4.4 (Lozano-Robledo [LR13, Lemma 6.6])**.** *Let H be a nontrivial subgroup of NC_s that fixes each element of a one-dimensional subspace L of $E_0[p]$. Then one of the following holds:*

(i) *H is contained in the subgroup $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \,\middle|\, b \in \mathbb{F}_p^\times \right\}$ and $V = L_1$.*

(ii) *H is contained in the subgroup* $\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{F}_p^\times \right\}$ *and* $V = L_2$.

(iii) $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & c \\ c^{-1} & 0 \end{pmatrix} \middle| \, \text{for some } c \text{ in } \mathbb{F}_p^\times \right\}$ *and* $V = \langle (c,1) \rangle$.

Suppose we are in Case (i) of Lemma 4.4. Let g be a generator of the (unique, cyclic) subgroup of $\mathbb{F}_p^\times$ of order $\frac{p-1}{i(p)}$, and let $M_g \in G$ be such that $\det(M_g) = g$.

First suppose $M_g \in C_s$, say $M_g = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Since G is not contained in C_s, there is also a matrix $A \coloneqq \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} \in G$, and so

$$\begin{pmatrix} 0 & d^{-1} \\ c^{-1} & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} \in G$$

and thus also

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} = \begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix} \in G.$$

Let $Z \coloneqq \left\langle \begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix} \right\rangle$. Then $Z \subset G$ and $Z \cap H = \{e\}$, so

$$\frac{p-1}{d_0} \, \Big| \, \frac{p-1}{i(p)} \, \Big| \, [G:H] = [F_0(P) : F_0],$$

so

$$p - 1 \mid [F_0(P) : \mathbb{Q}].$$

Now suppose $M_g \in NC_s \backslash C_s$, say $M_g = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}$. Then $\det M_g = -cd$, so $cd = -g$. Also $M_g^2 = \begin{pmatrix} -g & 0 \\ 0 & -g \end{pmatrix} \in G$. Let $W \coloneqq \left\langle \begin{pmatrix} -g & 0 \\ 0 & -g \end{pmatrix} \right\rangle$. Then $\frac{p-1}{2i(p)} \mid \#W$ and $W \cap H = \{e\}$, so reasoning as above we get

$$\frac{p-1}{2} \mid [F_0(P) : \mathbb{Q}].$$

The analysis for Case (ii) of Lemma 4.4 is exactly as for Case (i).

Suppose we are in case (iii) of Lemma 4.4. Then $\#\rho_p(\mathfrak{g}_F) \mid 2$. As above, d_0 times the order of $\det \rho_p(\mathfrak{g}_{F_0})$ is divisible by $p-1$, so

$$p - 1 \mid d_0[G:H] \mid 2[F_0(P) : \mathbb{Q}].$$

Conclusion: in Case 2, we may take $c = 2$.

4.2.3. *Case 3.* A nonsplit Cartan subgroup C_{ns} of $\mathrm{GL}(E_0[p])$ is obtained by endowing $E_0[p]$ with the structure of a 1-dimensional vector space over $\mathbb{F}_{p^2}$ and taking the group of $\mathbb{F}_{p^2}$-linear automorphisms. It is known that all such groups are conjugate in $\mathrm{GL}(E_0[p])$ and that the normalizer of C_{ns} consists of all $\mathbb{F}_{p^2}$ *semi*linear automorphisms of $\mathrm{GL}(E_0[p])$ and has order $2(p^2-1)$. But we have already recalled more than we need, in view of the following result ([LR13, Lemma 7.4]).

Lemma 4.5. *Let NC_{ns} be the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}(E_0[p])$, and let $H \subset NC_{\mathrm{ns}}$ be a subgroup that fixes each element in a one-dimensional $\mathbb{F}_p$-subspace of $E_0[p]$. Then $\#H \leq 2$.*

Therefore for a nonzero $P \in E_0[P]$, we have

$$\frac{p-1}{2i(p)} \mid \frac{p-1}{2d_0} \mid [G:H] = [F_0(P):F_0],$$

so $\frac{p-1}{2} \mid [F_0(P):\mathbb{Q}]$ and we may take $c = 2$.

4.2.4. *Case 4.* We will use the following result of Etropolski, based on work of Serre and an observation of Mazur.

Proposition 4.6 ([Et16, Prop. 2.6])**.** *Let $E_{/K_0}$ be an elliptic curve defined over a number field K_0 of degree d_0. For a prime number p, let $\overline{G}$ be the projective image of the mod p Galois representation.*

a) *If $\overline{G} \cong A_4$, then $p \leq 9d_0 + 1$.*
b) *If $\overline{G} \cong S_4$, then $p \leq 12d_0 + 1$.*
c) *If $\overline{G} \cong A_5$, then $p \leq 15d_0 + 1$.*

So this case can occur only if $p \leq 15d_0 + 1$; by Remark 3.1 we can omit these primes.

4.2.5. *Case 5.* The subgroup G is contained in a Borel subgroup iff E admits an F_0-rational p-isogeny. Our assumption $\mathrm{SI}(d_0)$ is precisely that the set of primes p for which there is a non-CM elliptic curve defined over a number field of degree d_0 together with a rational point of order p is finite, so by Remark 3.1 we can omit these primes. This completes the proof of part a).

4.2.6. *The proof of part b).* The hypothesis $\mathrm{SI}(d_0)$ was only used in Case 5, so only Case 5 needs to be redone under the hypotheses of part b): suppose that F_0 does not contain the Hilbert class field of any imaginary quadratic field. (This hypothesis precisely prohibits having an elliptic curve $E_{/F_0}$ for which the CM is F_0-rationally defined.) Then Larson-Vaintrob showed [LV14] that, assuming (GRH), the set of primes p such that an elliptic curve $E_{/F_0}$ admits an F-rational p-isogeny is bounded, giving Case 5 under (GRH). Finally, suppose moreover that $[F_0 : \mathbb{Q}] = 2$. Then the hypothesis on F_0 becomes that F_0 is not itself an imaginary quadratic field of class number 1, and under this hypothesis Momose showed [Mo95] that the set of primes p such that an elliptic curve $E_{/F_0}$ admits an F-rational p-isogeny is finite. This completes the proof of Case 5 and thus the proof of Theorem 4.3b).

References

[BCP17] A. Bourdon, P.L. Clark and P. Pollack, *Anatomy of torsion in the CM case*. Math. Z. 285 (2017), 795-820.

[CA] P.L. Clark, *Commutative algebra*. Available online at `http://math.uga.edu/~pete/integral2015.pdf`.

[CP15] P.L. Clark and P. Pollack, *The truth about torsion in the CM case*. C. R. Math. Acad. Sci. Paris 353 (2015), 683–688.

[CP17a] ———, *The truth about torsion in the CM case, (II)*. Q. J. Math. 68 (2017), 1313–1333.

[CP17b] ———, *Pursuing polynomial bounds on torsion*. To appear in Israel J. Math.

[CX08] P.L. Clark and X. Xarles, *Local bounds for torsion points on abelian varieties* Canad. J. Math. 60 (2008), 532–555.

[Et16] A. Etropolski, *Local-global principles for certain images of Galois representations*. Preprint online at `http://math.rice.edu/~ae22/Papers/localglobal.pdf`.

[EW80] P. Erdős and S.S. Wagstaff Jr., *The fractional parts of the Bernoulli numbers*. Illinois J. Math 24 (1980), 104–112.

[FJ] M.D. Fried and M. Jarden, *Field arithmetic*. Third edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, Berlin, 2008.

[Fr97] S. Friedland, *The maximal orders of finite subgroups in $GL_n(\mathbb{Q})$*. Proc. Amer. Math. Soc. 125 (1997), 3519–3526.

[GK16] R. Guralnick and K. Kedlaya, *Endomorphism fields of abelian varieties*. Preprint online at `http://arxiv.org/abs/1606.02803v1`.

[GR17] É. Gaudron et G. Rémond, *Torsion des variétés abéliennes CM*. To appear in Proc. AMS.

[HS99] M. Hindry and J. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique*. C. R. Acad. Sci. Paris Sér. I Math. 329 (1999), 97–100.

[KA79] S.L. Kleiman and A.B. Altman, *Bertini theorems for hypersurface sections containing a subscheme*. Comm. Algebra 7 (1979), 775–790.

[KK96] C.H. Kim and J.K. Koo, *On the genus of some modular curves of level N*. Bull. Austral. Math. Soc. 54 (1996), 291–297.

[LR13] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*. Math. Ann. 357 (2013), 279–305.

[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.

[Mi] J. Milne, *Complex Multiplication*. Online notes; available at `http://www.jmilne.org/math/CourseNotes/CM.pdf`.

[Mi87] H. Minkowski, *Zur Theorie der positiven quadratische Formen*, J. reine angew. Math. 101 (1887), 196–202.

[Mo95] F. Momose, *Isogenies of prime degree over number fields*. Compositio Math. 97 (1995), 329–348.

[Ols74] L. Olson, *Points of finite order on elliptic curves with complex multiplication*. Manuscripta Math. 14 (1974), 195–205.

[Po04] B. Poonen, *Bertini theorems over finite fields*. Ann. of Math. (2) 160 (2004), 1099–1127.

[RA] J.L. Ramírez Alfonsín, *The Diophantine Frobenius Problem*. Oxford University Press, Oxford, 2005.

[Re17] G. Rémond, *Degré de définition des endomorphismes d'une variété abélienne*. Preprint at `http://www-fourier.ujf-grenoble.fr/~remond/4441.pdf`.

[Se72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. 15 (1972), 259–331.

[Sh] G. Shimura, *Abelian varieties with complex multiplication and modular functions*. Princeton Mathematical Series 46. Princeton University Press, Princeton, NJ, 1998.

[Si86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, 1986.

[Si88] A. Silverberg, *Torsion points on abelian varieties of CM-type*. Compositio Math. 68 (1988), 241–249.

[Si92a] ———, *Points of finite order on abelian varieties*. In p-adic methods in number theory and algebraic geometry, 175–193, Contemp. Math. 133, American Mathematical Society, Providence, RI, 1992.

[Si92b] ———, *Fields of definition for homomorphisms of abelian varieties*. J. Pure Appl. Algebra 77 (1992), 253–262.