

RESEARCH ARTICLE

Torsion and twists of abelian varieties

Mentzelos Melistas^{1,2} ¹Faculty of Mathematics and Physics,
Department of Algebra, Charles
University, Praha, Czech Republic²Department of Applied Mathematics,
University of Twente, Enschede, The
Netherlands**Correspondence**Mentzelos Melistas, Department of
Algebra, Faculty of Mathematics and
Physics, Charles University, Sokolovská
83, 18600 Praha 8, Czech Republic.
Email: mentzmel@gmail.com**Funding information**Czech Science Foundation, Grant/Award
Number: 21-00420M**Abstract**

In this article, we investigate the possible torsion subgroups of twists of abelian varieties with good reduction. As an application, we prove a theorem concerning ramified primes over any quadratic extension where odd-order torsion growth is achieved. In particular, we show that for every rational elliptic curve and every imaginary quadratic field not equal to $\mathbb{Q}(\sqrt{-3})$ satisfying the Heegner hypothesis, no odd-order torsion growth can occur.

MSC 2020

11G05, 11G07, 11G10 (primary), 14H52, 14K15 (secondary)

1 | INTRODUCTION

Let K be a number field of degree d and let A/K be an abelian variety of dimension g . The Mordell–Weil theorem states that the set $A(K)$ of K -rational points of A/K is a finitely generated abelian group, and therefore, it decomposes as

$$A(K) \cong A(K)_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $A(K)_{\text{tors}}$ is a finite subgroup called the torsion subgroup and r is a nonnegative integer. The problem of producing bounds for the torsion subgroup $A(K)_{\text{tors}}$ has a very long and rich history. When $g = 1$ and $d \leq 2$, that is, when K is either \mathbb{Q} or a quadratic number field and A/K is an elliptic curve defined over K , we have a complete classification of the possible torsion subgroups that can occur (see [14, 22], and [15]). For higher degree d , the uniform boundedness theorem, due to Merel [28], tells us that for every $d > 0$, there exists a bound $B(d)$ such that for every number field K of degree d and every elliptic curve E/K , we have that

$$|E(K)_{\text{tors}}| < B(d).$$

For higher dimensional abelian varieties, a lot less is known. For example, even for abelian surfaces A/\mathbb{Q} , there is no known uniform bound for the group $A(\mathbb{Q})_{\text{tors}}$.

Given an abelian variety A/K , it is natural to ask how the torsion subgroup $A(K)_{\text{tors}}$ changes upon quadratic twisting. More specifically, let $K(\sqrt{d})$ be a quadratic extension of K , for some element d of K , and denote by A^d/K the quadratic twist of A/K by d (see Example 2.3 below for the definition). One can then ask the following.

Question 1. *If $A(K)_{\text{tors}} \neq A^d(K)_{\text{tors}}$, then are there any properties (depending on A/K) that the extension $K(\sqrt{d})/K$ must necessarily have?*

We also refer the reader to [39], which contains related results, including the statement that over a number field, an abelian variety has only finitely many twists that admit a K -rational torsion point of order strictly greater than 2. In this article, we will primarily be interested in the relationship between the primes of K that ramify in $K(\sqrt{d})$ and the primes of good reduction of A/K . In fact, we are able to prove a more general theorem concerning twists of A/K by irreducible rational representations, assuming certain ramification conditions on K . Our methods are local relying on the interplay between torsion points and reduction properties of abelian varieties (see [6] and [27] for more on this relationship).

Let K be a field, let L/K be a finite Galois extension with Galois group denoted by G , and let A/K be an abelian variety. The group algebra $\mathbb{Q}[G]$ decomposes as a direct sum

$$\mathbb{Q}[G] = \bigoplus_{\rho} \mathbb{Q}[G]_{\rho},$$

where the direct sum is indexed by the irreducible rational representations of G and $\mathbb{Q}[G]_{\rho}$ is the ρ -isotypic component of $\mathbb{Q}[G]$. If

$$I_{\rho} = \mathbb{Q}[G]_{\rho} \cap \mathbb{Z}[G],$$

then we can construct (see Definition 2.1 below) an abelian variety defined over K denoted by

$$A_{\rho} := I_{\rho} \otimes_{\mathbb{Z}} A$$

and called the ρ -twist of A/K . Such twists were considered by Mazur and Rubin [23, 24] in order to study Selmer ranks of elliptic curves. We will not consider Selmer ranks in this article, but we expect that our results will have applications to Selmer groups of quadratic twists of abelian varieties.

Our first result concerns the possible orders of K -rational torsion points of A_{ρ} , under certain assumptions on K and A/K .

Theorem 1.1. *Let K be a local field of characteristic 0 with valuation v_K and residue field k of characteristic $p > 2$. Let A/K be a simple g -dimensional abelian variety that has good reduction and let L/K be a totally ramified finite Galois extension of degree $m \geq 2$ with Galois group G . Then*

- (i) *If ρ is a nontrivial irreducible rational representation of G and $v_K(p) < \frac{p-1}{m}$, then the twist A_{ρ}/K cannot have any K -rational points of order p .*

(ii) If ρ is a nontrivial irreducible rational representation of G and the twist A_ρ/K has a K -rational point of prime order ℓ with $\ell \neq p$, then $\ell \leq 2g + 1$.

Remark 1.2. Example 2.9 below shows that the assumption that $v_K(p) < \frac{p-1}{m}$ in Part (i) of Theorem 1.1 is necessary and cannot be removed. The assumption that A/K has good reduction in Theorem 1.1 is also necessary and cannot be removed. The latter is, of course, expected because every elliptic curve over \mathbb{Q} is a quadratic twist of another elliptic curve defined over \mathbb{Q} .

As an application of Theorem 1.1, we obtain the following theorem.

Theorem 1.3. *Let A/\mathbb{Q} be a simple g -dimensional abelian variety of conductor N and let d be a square-free integer. If d has a prime divisor $p > 3$ with $p \nmid N$, then the quadratic twist A^d/\mathbb{Q} cannot have any \mathbb{Q} -rational points of prime order ℓ with $\ell > 3$.*

Remark 1.4. The above theorem partially generalizes [26, Theorem 1.2, Part (i)] and can also be thought of as a higher dimensional analog of a proposition of Mazur and Gouvêa [12, Proposition 1]. Moreover, as is shown in [26, Remark 1.4] if $d = -1$, then the conclusion of Theorem 1.3 does not hold.

We now explain some applications of Theorem 1.1 to torsion growth of abelian varieties over quadratic extensions. Let A/K be an abelian variety over a number field K and let L/K be a quadratic extension. If $A(L)_{\text{tors}} \setminus A(K)_{\text{tors}}$ contains a point of prime order p , then it follows from the Néron–Ogg–Shafarevich criterion [33, Theorem 1] that the primes of K that ramify in L are contained in the set

$$\{\mathfrak{p} \text{ is a prime of } \mathcal{O}_K : \mathfrak{p} \text{ lies above } p \text{ or } A/K \text{ has bad reduction at } \mathfrak{p}\}.$$

The following theorem tells us that under a certain assumption on the field K , every prime that ramifies in L and lies above p must be a prime of bad reduction of A/K .

Theorem 1.5. *Let A/K be a simple abelian variety over a number field K and let L be a quadratic extension of K . Assume that $A(L)_{\text{tors}} \setminus A(K)_{\text{tors}}$ contains a point of prime order p . If for all primes \mathfrak{p} of \mathcal{O}_K with associated valuation $v_{\mathfrak{p}}$, we have that $v_{\mathfrak{p}}(p) < \frac{p-1}{2}$, then the primes of K that ramify in L are contained in*

$$\{\mathfrak{p} \text{ is a prime of } \mathcal{O}_K : A/K \text{ has bad reduction at } \mathfrak{p}\}.$$

We note that Theorem 1.5 is sharp in the sense that the condition $v_{\mathfrak{p}}(p) < \frac{p-1}{2}$ is optimal (see Example 3.1 below).

Finally, we turn our attention to elliptic curves E/\mathbb{Q} and quadratic extensions L that satisfy the Heegner hypothesis for E/\mathbb{Q} , that is, L is an imaginary quadratic field and all prime divisors of the conductor N of E/\mathbb{Q} split in L . Under this assumption, we show that if $L \neq \mathbb{Q}(\sqrt{-3})$, then the quotient $|E_L(L)_{\text{tors}}|/|E(\mathbb{Q})_{\text{tors}}|$ is a power of 2 (see Corollary 3.8 below).

2 | TWISTS OF ABELIAN VARIETIES

In this section, we prove Theorem 1.1 and then derive some corollaries on torsion points of quadratic twists. Before we begin our proof, we recall some background material on twists of abelian varieties. We refer the reader to [25, 34] and [29] for further information concerning this topic.

Let K be any field, let A/K be an abelian variety, and let L/K be a finite Galois extension. If X/K is any abelian variety, then we will denote by X_L/L the base change of X/K to L . An L/K -form of the abelian variety A/K is a pair (B, ψ) , where B/K is an abelian variety and $\psi : A_L \rightarrow B_L$ is an isomorphism that is defined over L . Two L/K -forms (B, ψ) and (B', ψ') are called equivalent if they are isomorphic over K .

If (B, ψ) is an L/K -form of A/K , then the class of the map $\xi : \text{Gal}(L/K) \rightarrow \text{Aut}_L(A_L)$ given by $\xi(\sigma) = \psi^{-1} \circ \psi^\sigma$ for all $\sigma \in \text{Gal}(L/K)$ is an element of $H^1(\text{Gal}(L/K), \text{Aut}_L(A_L))$, that is, ξ is a 1-cocycle for $\text{Gal}(L/K)$ with values in $\text{Aut}_L(A_L)$. This association induces a bijection between the set of L/K -forms modulo equivalence and the pointed set $H^1(\text{Gal}(L/K), \text{Aut}_L(A_L))$ (see [32, Chapter III]).

To ease notation in what follows we shall write $\text{Aut}_L(A^n)$ for $\text{Aut}_L((A_L)^n)$ for every positive integer n .

Definition 2.1. Let A/K be an abelian variety and let R be a commutative ring with a ring homomorphism $R \rightarrow \text{End}_K(A)$. Fix a positive integer n . Let I be a finitely generated free R -module of rank n with a continuous right action of the absolute Galois group of K and fix an R -module isomorphism $\psi : R^n \rightarrow I$. If $\text{GL}_n(R)$ is regarded as a subgroup of $\text{Aut}_L(A^n)$, then the homomorphism $\xi : G \rightarrow \text{Aut}_L(A^n)$ given by $\xi(\sigma) = \psi^{-1} \circ \psi^\sigma$ is a 1-cocycle for $\text{Gal}(L/K)$, that is, the class of ξ belongs to $H^1(\text{Gal}(L/K), \text{Aut}_L(A^n))$. Therefore, there exists an abelian variety $(I \otimes_R A)/K$ corresponding to ξ . We call the abelian variety $(I \otimes_R A)/K$ the twist of A/K by I .

Note that according to Definition 2.1, the variety $(I \otimes_R A)/K$ is an L/K -form of A^n/K . Moreover, it is shown in [25, Remark 1.2] that the definition of the twist is independent of the choice of ψ . We proceed with two important examples that will be used below.

Example 2.2 (Weil restriction). Let L/K be a finite extension and let B/L be an abelian variety. Recall that the Weil restriction $\text{Res}_{L/K}(B)$ of B/L from L to K is the scheme defined over K representing the functor from K -schemes to sets given by $S \mapsto B(S \times_K L)$.

Let L/K be a finite Galois extension with $G = \text{Gal}(L/K)$ and let $I = R[G]$. Then the twist $I \otimes_R B$ is isomorphic to $\text{Res}_{L/K}(B)$ (see [25, Proposition 4.1]).

Example 2.3 (Quadratic twists, see also [34, Section 3.1.3]). Let A/K be an abelian variety over a field K and let $L = K(\sqrt{d})$ be a quadratic extension. Let $\chi_L : G_K \rightarrow \{\pm 1\}$ be the unique nontrivial quadratic character of the absolute Galois group G_K of K that factors through $\text{Gal}(L/K)$. Let $R = \mathbb{Z}$ considered as a subset of $\text{End}_K(A)$ via the identification of R with $\{[m] : m \in \mathbb{Z}\}$, where $[m]$ in the multiplication by m on A/K . Consider I to be a free rank 1 module over \mathbb{Z} equipped by an action of G_K given by $i^\sigma = \chi_L(\sigma) \cdot i$ for $i \in I$ and $\sigma \in G_K$. Denote by A^d/K the abelian variety $(I \otimes_R A)/K$. Here, the map ψ is defined as follows; fix a generator i_0 of I and let $\psi : R \rightarrow I$ be the isomorphism given by $\psi(m) = m \cdot i_0$. The associated 1-cocycle is $\xi : \text{Gal}(L/K) \rightarrow \text{Aut}_L(A)$ given

by $\xi(\gamma) = [-1]$ and $\xi(\text{id}) = [1] = \text{id}$, where γ is the generator of $\text{Gal}(L/K)$. The abelian variety A^d/K is called the quadratic twist of A/K by d .

In the special case where E/K is an elliptic curve and $\text{char}(K) \neq 2, 3$ using [35, Example X.2.4], we see that E^d/K is the usual quadratic twist of E/K by d , that is, if E/K is given by a short Weierstrass equation

$$y^2 = x^3 + ax + b,$$

for some $a, b \in K$, then E^d/K is given by a short Weierstrass equation

$$dy^2 = x^3 + ax + b.$$

Consider now a finite Galois extension L/K with Galois group $G := \text{Gal}(L/K)$. The group algebra $\mathbb{Q}[G]$ decomposes as a direct sum $\mathbb{Q}[G] = \bigoplus_{\rho} \mathbb{Q}[G]_{\rho}$, where the direct sum is indexed by the irreducible rational representations of G and $\mathbb{Q}[G]_{\rho}$ is the ρ -isotypic component of $\mathbb{Q}[G]$.

Definition 2.4. Let A/K be an abelian variety. If ρ is an irreducible rational representation of the group G , then let

$$I_{\rho} = \mathbb{Q}[G]_{\rho} \cap \mathbb{Z}[G].$$

Define the ρ -twist of A/K by

$$A_{\rho} := I_{\rho} \otimes_{\mathbb{Z}} A.$$

The following theorem, due to Mazur, Rubin, and Silverberg, will be very useful in the proof of Theorem 1.1.

Theorem 2.5 (See [25, Theorem 4.5]). *Let L/K be a finite Galois extension with Galois group G and let A/K be an abelian variety. Then $\text{Res}_{L/K}(A_L)$ is isogenous over K to $\prod_{\rho} A_{\rho}$, where the product is taken over all irreducible rational representations of G .*

Before we proceed to the proof of Theorem 1.1, we need to briefly recall a few basic facts concerning reduction of abelian varieties. The interested reader can find more information on this topic in [2] and [20]. Let K be a local field, that is, K is a complete field with respect to a discrete valuation v_K and has finite residue field k , and let A/K be an abelian variety of dimension g . We denote by $\mathcal{A}/\mathcal{O}_K$ the Néron model of A/K . The special fiber \mathcal{A}_k/k of $\mathcal{A}/\mathcal{O}_K$ is a smooth commutative group scheme. We denote by \mathcal{A}_k^0/k the connected component of the identity of \mathcal{A}_k/k . By a theorem of Chevalley (see [8, Theorem 1.1]), there exists a short exact sequence

$$0 \longrightarrow T \times U \longrightarrow \mathcal{A}_k^0 \longrightarrow B \longrightarrow 0,$$

where T/k is a torus, U/k is a unipotent group, and B/k is an abelian variety. The number $\dim(U)$ (resp. $\dim(T)$, $\dim(B)$) is called the unipotent (resp. toric, abelian) rank of A/K . By construction, we have the following equality $g = \dim(U) + \dim(T) + \dim(B)$. We say that A/K has purely additive reduction if $g = \dim(U)$, or equivalently, if $\dim(T) = \dim(B) = 0$.

Proof of Theorem 1.1. To ease notation, let ρ_0, \dots, ρ_n be the irreducible rational representations of G with ρ_0 the trivial representation (corresponding to the trivial twist of A/K) and let $A_i := A_{\rho_i}$ for $i = 1, \dots, n$. \square

Lemma 2.6. *For every $i = 1, \dots, n$, the abelian variety A_i has purely additive reduction.*

Proof Lemma 2.6. Let $W := \text{Res}_{L/K}(A_L)$ be the Weil restriction of the base change A_L/L of A/K to L . Theorem 2.5 tells us that there exists an isogeny $W \rightarrow A \times A_1 \times \dots \times A_n$ defined over K . Since L/K is totally ramified and A/K has good reduction, using [29, Remark on Page 179], we obtain that the abelian rank of W/K is equal to the dimension of A/K and that the toric rank of W/K is zero. Recall that we assume that A/K has good reduction. This implies that the abelian rank of A/K is equal to the dimension of A/K . Denote by $\mathcal{A}/\mathcal{O}_K$ the Néron model of A/K and by $\mathcal{A}_i/\mathcal{O}_K$ the Néron model of A_i/K , for every $i = 1, \dots, n$. Since the Néron model of $(A \times A_1 \times \dots \times A_n)/K$ is $(A \times A_1 \times \dots \times A_n)/\mathcal{O}_K$ and the abelian, unipotent, and toric ranks of abelian varieties are preserved under isogeny (see [1, Corollaire IX.2.2.7]), we find that A_i/K has purely additive reduction for every $i = 1, \dots, n$. This proves our lemma. \square

Proof of Part (i): Assume that for some $j > 0$ the twist A_j/K has a K -rational point of order p and we will arrive at a contradiction. Since A_j/K acquires good reduction in L (because it is an L/K -form of A/K) and $v_K(p) < \frac{p-1}{m}$, using [27, Theorem 1.1], applied to the base extension of A_j/K to the maximal unramified extension of K , we find that A_j/K cannot have purely additive reduction. However, this contradicts Lemma 2.6. This proves part (i).

Proof of Part (ii): Assume that for some $j > 0$, the twist A_j/K has a K -rational point of order ℓ with $\ell \neq p$. We need to show that $\ell \leq 2g + 1$, where g is the dimension of A/K . Using Lemma 2.6, we find that A_j/K has purely additive reduction. Therefore, using [6, Main Theorem Part (iii)], we find that $\ell \leq 2g + 1$. This completes the proof of Theorem 1.1.

Remark 2.7. If L/K is a finite abelian Galois extension, then the irreducible rational representations of $\text{Gal}(L/K)$ are in one-to-one correspondence with the cyclic subextensions of K in L . Assume now that L/K is a quadratic extension with Galois group G and denote by σ the generator of G . According to [34, Section 5.3], if ρ_L is the irreducible rational representation corresponding to the extension L/K , then $\mathbb{Z}[G]_{\rho_L} = (\sigma - 1)\mathbb{Z}$ is a free rank one \mathbb{Z} -module. Moreover, if $\chi_L : G_K \rightarrow \{\pm 1\}$ is the unique nontrivial quadratic character of the absolute Galois group G_K of K that factors through $\text{Gal}(L/K)$, then every $\gamma \in G_K$ acts on $\mathbb{Z}[G]_{\rho_L}$ as multiplication by $\chi_L(\gamma)$. Therefore, it follows that the corresponding abelian variety A_{ρ_L}/K is just the quadratic twist A^d/K of Example 2.3, for some $d \in L$ with $L = K(\sqrt{d})$.

Example 2.8 (See also the [MathOverflow post](#) [21]) In this example, we show that it is possible for both an elliptic curve and a quadratic twist of it to have rational points of odd orders. Let E/\mathbb{Q} be the elliptic curve given by the following Weierstrass equation:

$$y^2 + xy + y = x^3 - 76x + 298.$$

The curve E/\mathbb{Q} has LMFDB [18] label 50a2 and $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Therefore, we see that $E(\mathbb{Q}_5)$ contains a point of order 3. Using SAGE [37], we find that the quadratic twist of E/\mathbb{Q} by 5, which we

denote by E^5/\mathbb{Q} , has Weierstrass equation

$$y^2 + xy + y = x^3 + x^2 - 3x + 1$$

and LMFDB [18] label 50b3. Moreover, we have that $E^5(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$. Therefore, we see that $E^5(\mathbb{Q}_5)$ contains a point of order 5. Thus, both the curve E/\mathbb{Q}_5 and the curve E^5/\mathbb{Q}_5 have (nontrivial) \mathbb{Q}_5 -rational points of finite order.

Example 2.9. This example shows that the condition $v_K(p) < \frac{p-1}{m}$ in Theorem 1.1 is necessary, with $p = 3$ and $m = 2$. Consider the elliptic curve E/\mathbb{Q} given by the following Weierstrass equation:

$$y^2 + y = x^3 + x^2 - 9x - 15.$$

The curve E/\mathbb{Q} has LMFDB [18] label 19a2. Therefore, the base change $E_{\mathbb{Q}_3}/\mathbb{Q}_3$ has good reduction. Using SAGE [37], we find that the quadratic twist of E/\mathbb{Q} by -3 , which we denote by E^{-3}/\mathbb{Q} , has Weierstrass equation

$$y^2 + y = x^3 - 84x + 315$$

and LMFDB [18] label 171b2. Moreover, we have that $E^{-3}(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. This implies that the curve $E_{\mathbb{Q}_3}^{-3}/\mathbb{Q}_3$ has a \mathbb{Q}_3 -rational point of order 3.

Corollary 2.10. *Let K be a number field, let A/K be a simple abelian variety, and let $L = K(\sqrt{d})$ be a quadratic extension of K , for some $d \in K$. Fix a rational prime p . Let \mathfrak{P} be a prime of K that lies above p and denote by $v_{\mathfrak{P}}$ the corresponding valuation of K . Assume that \mathfrak{P} ramifies in L and that A/K has good reduction modulo \mathfrak{P} . If $v_{\mathfrak{P}}(p) < \frac{p-1}{2}$, then the quadratic twist A^d/K cannot have a K -rational point of order p .*

Proof. Since L/K is a quadratic extension and we assume that \mathfrak{P} ramifies in L , we know that there exists a unique prime \mathfrak{P}' of L that lies above \mathfrak{P} . Let $K_{\mathfrak{P}}$ be the completion of K at \mathfrak{P} and let $L_{\mathfrak{P}'}$ be the completion of L at \mathfrak{P}' . It follows from basic algebraic number theory (see [31, Chapter II]) that under our assumptions, the extension $L_{\mathfrak{P}'}/K_{\mathfrak{P}}$ is a (totally) ramified quadratic extension of local fields. Consider the base change $A_{K_{\mathfrak{P}}}/K_{\mathfrak{P}}$ of A/K to $K_{\mathfrak{P}}$. Using Paragraph 2.7, we see that Part (i) of Theorem 1.1 implies that the abelian variety $A_{K_{\mathfrak{P}}}^d/K_{\mathfrak{P}}$ cannot have a $K_{\mathfrak{P}}$ -rational point of order p . Therefore, we find that A^d/K cannot have a K -rational point of order p . This proves our corollary. □

As an application of the previous corollary, we will now prove Theorem 1.3 of the introduction. Before we proceed to our proof, we need to recall the following useful lemma.

Lemma 2.11. *Let K be a field with $\text{char}(K) \neq 2$ and let A/K be a simple abelian variety. Let L/K be an abelian Galois extension of degree $m > 1$ and assume that the exponent of the Galois group $\text{Gal}(L/K)$ is 2. Then there exist $d_i \in K$ for $i = 1, \dots, m$ with associated quadratic twists $A_i := A^{d_i}$*

and a group homomorphism

$$\bigoplus_{i=1}^m A_i(K) \longrightarrow A_L(L),$$

whose kernel and cokernel are annihilated by m .

Proof. Using [16, Page 165], we find that this is a special case of [16, Lemma 1.1] with $e = 2$. \square

When $m = 2$, which is the case of primary interest for us, we immediately obtain the following corollary.

Corollary 2.12. *Let L/K be a quadratic extension of number fields with $L = K(\sqrt{d})$ and let A/K be a simple abelian variety. If n is odd, then*

$$A(K)[n] \oplus A^d(K)[n] \cong A_L(L)[n].$$

We are now ready to proceed with our proof.

Proof of Theorem 1.3. Assume that the twist A^d/\mathbb{Q} has a \mathbb{Q} -rational point of prime order ℓ for some $\ell > 3$, and we will find a contradiction. Recall that we assume the existence of a prime $p > 3$ that divides d but it does not divide N .

Assume first that $\ell \neq p$. Since p and N are coprime, we see that A/\mathbb{Q} has good reduction modulo p . Fix an algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} . Let $K_\ell = \mathbb{Q}(A[\ell])$ be the ℓ -division field of A/K , that is, the minimal field of definition of all the ℓ -torsion points of $A(\overline{\mathbb{Q}})$. If $L = \mathbb{Q}(\sqrt{d})$, then it follows from Corollary 2.12 that

$$A(\mathbb{Q})[\ell] \oplus A^d(\mathbb{Q})[\ell] \cong A_L(L)[\ell].$$

Since we assume that A^d/\mathbb{Q} has a \mathbb{Q} -rational point of order ℓ , we find that A_L/L has an L -rational point of order ℓ . Therefore, we have that $L \subseteq K_\ell$. On the other hand, since A/\mathbb{Q} has good reduction modulo p , using the Néron–Ogg–Shafarevich criterion [33, Theorem 1], we find that p is unramified in K_ℓ . However, this contradicts the fact that $L \subseteq K_\ell$ because p divides d , and hence, it ramifies in L .

Assume now that every prime divisor of d divides ℓ , that is, that $d = \pm \ell$. Since $\ell \geq 5$, we see that if v_ℓ is the valuation corresponding to ℓ , then $v_\ell(\ell) = 1 < \frac{\ell-1}{2}$. Therefore, applying Corollary 2.10 (for $K = \mathbb{Q}$ and $\ell = \mathfrak{P}$), we find that A^d/\mathbb{Q} cannot have a \mathbb{Q} -rational point of order ℓ , which is again a contradiction. This proves our theorem. \square

Remark 2.13. Let R be a complete discrete valuation ring with fraction field K of characteristic $p > 0$ and algebraically closed residue field. One may wonder whether there can exist an analog of Theorem 1.1 over the field K . Unfortunately, such an analog does not seem to exist, as we now explain. Let E/K be an elliptic curve with good reduction and let \mathcal{E}/R be the Néron Model of E/K . Assume that the Hasse invariant of \mathcal{E}/R has vanishing order $\frac{p-1}{2}$ (see [17, Section 5] for information on the Hasse invariant of \mathcal{E}/R). Let $E^{(p)}/K$ be the Frobenius pullback of the curve E/K , which still has good reduction by [17, Proposition 7.2]. According to [17, Proposition 8.3] for

every separable quadratic extension K'/K , the corresponding quadratic twist $\widetilde{E^{(p)}}/K$ of $E^{(p)}/K$ has a K -rational point of order p .

3 | TORSION GROWTH OF ABELIAN VARIETIES AND AN APPLICATION TO A CONJECTURE OF GROSS AND ZAGIER

In this section, we consider torsion growth questions for abelian varieties over quadratic fields. After proving Theorem 1.5, we turn to elliptic curves E/\mathbb{Q} and we study the possible torsion growth over quadratic extensions satisfying the Heegner hypothesis with respect to E/\mathbb{Q} .

Proof of Theorem 1.5. Let \mathfrak{p} be a prime of \mathcal{O}_K that ramifies in L and lies above p . Assume that A/K has good reduction modulo \mathfrak{p} and we will find a contradiction. Write $L = K(\sqrt{d})$ for some $d \in K$ and denote by $v_{\mathfrak{p}}$ the valuation associated to \mathfrak{p} . Since we assume that $v_{\mathfrak{p}}(p) < \frac{p-1}{2}$, using Corollary 2.10, we find that the twist A^d/K cannot have a K -rational point of order p . However, this is a contradiction because by Corollary 2.12, we have that

$$A(K)[p] \oplus A^d(K)[p] \cong A_L(L)[p],$$

and we assume that $A(L)_{\text{tors}} \setminus A(K)_{\text{tors}}$ contains a point of order p . This proves our theorem. \square

Example 3.1. This example shows that Theorem 1.5 is sharp for $p := 7$. Consider the elliptic curve E/\mathbb{Q} with LMFDB [18] label 26.b1. This elliptic curve is given by the following Weierstrass equation:

$$y^2 + xy + y = x^3 - x^2 - 213x - 1257.$$

Let $\mathbb{Q}(\zeta_7)^+$ be the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_7)$. Using the LMFDB database, we find that $E_{\mathbb{Q}(\zeta_7)^+}(\mathbb{Q}(\zeta_7)^+)_{\text{tors}}$ is trivial and that $E_{\mathbb{Q}(\zeta_7)}(\mathbb{Q}(\zeta_7))_{\text{tors}} \cong \mathbb{Z}/7\mathbb{Z}$. Thus, the curve $E_{\mathbb{Q}(\zeta_7)^+}/\mathbb{Q}(\zeta_7)^+$ acquires a torsion point of order 7 over the quadratic extension $\mathbb{Q}(\zeta_7)/\mathbb{Q}(\zeta_7)^+$. Moreover, if \mathfrak{p}^+ is the prime of $\mathbb{Q}(\zeta_7)^+$ that lies above 7, then the curve $E_{\mathbb{Q}(\zeta_7)^+}/\mathbb{Q}(\zeta_7)^+$ has good reduction modulo \mathfrak{p}^+ . Finally, if $v_{\mathfrak{p}^+}$ is the associated valuation, we see that $v_{\mathfrak{p}^+}(7) = \frac{7-1}{2}$.

Example 3.2. The following is an interesting example where an elliptic curve acquires both a torsion point of large order and everywhere good reduction over a quadratic extension. Consider the elliptic curve E/\mathbb{Q} with LMFDB [18] label 1225.b2. This elliptic curve is given by the following Weierstrass equation

$$y^2 + xy + y = x^3 + x^2 - 8x + 6.$$

Let $\mathbb{Q}(\zeta_{35})^+$ be the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{35})$. Recall that the degree of the extension $\mathbb{Q}(\zeta_{35})^+/\mathbb{Q}$ is 12. The field $\mathbb{Q}(\zeta_{35})^+$ contains a sextic number field K with defining polynomial

$$x^6 - x^5 - 7x^4 + 2x^3 + 7x^2 - 2x - 1.$$

Using SAGE [37] (or MAGMA), it is easy to see that the torsion subgroup $E_K(K)_{\text{tors}}$ is trivial and that E_K/K has bad reduction modulo two prime ideals. In fact, E_K/K is a twist of an elliptic curve that appears in [19, Section 7.2]. On the other hand, using LMFDB, we find that the curve $E_{\mathbb{Q}(\zeta_{35})^+}/\mathbb{Q}(\zeta_{35})^+$ has a torsion point of order 37 and everywhere good reduction.

For an elliptic curve E/\mathbb{Q} and quadratic field L , the relationship between $E(\mathbb{Q})_{\text{tors}}$ and $E_L(L)_{\text{tors}}$ has been studied by González-Jiménez and Tornero in [10] and [11]. Moreover, Najman, answering a problem posed by González-Jiménez and Tornero, in [30] gave sharp upper bounds on the number of quadratic extensions for which $E(\mathbb{Q})_{\text{tors}} \subsetneq E_L(L)_{\text{tors}}$. In the following theorem, we show that if every prime of bad reduction for E/\mathbb{Q} is unramified in L , then the possible torsion growth is very restricted.

Theorem 3.3. *Let E/\mathbb{Q} be an elliptic curve, let L/\mathbb{Q} be a quadratic extension, and assume that every prime of bad reduction of E/\mathbb{Q} is unramified in L . Then*

- (i) *The set $E_L(L)_{\text{tors}} \setminus E(\mathbb{Q})_{\text{tors}}$ cannot contain points of prime order $p > 3$.*
- (ii) *If there exists a prime $p \neq 3$, which ramifies in L , then the quotient $|E_L(L)_{\text{tors}}|/|E(\mathbb{Q})_{\text{tors}}|$ is equal to a power of 2.*

Proof. *Proof of Part (i):* This part follows directly from Theorem 1.5.

Proof of Part (ii): Using the previous part, we see that we only need to show that $E_L(L)_{\text{tors}} \setminus E(\mathbb{Q})_{\text{tors}}$ cannot contain a point of order 3. Assume that $E_L(L)_{\text{tors}} \setminus E(\mathbb{Q})_{\text{tors}}$ contains a point P of order 3, and we will find a contradiction. Write $L = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free. By Corollary 2.12, we have that $E_L(L)[3] \cong E(\mathbb{Q})[3] \oplus E^d(\mathbb{Q})[3]$, which implies that there exists a point $P' \in E^d(\mathbb{Q})[3]$ of order 3. Since p is a prime of good reduction for E/\mathbb{Q} and p divides d , we find that E^d/\mathbb{Q} has reduction of Kodaira type I_0^* , II, or I_8^* modulo p by [7, Proposition 1] and [7, Table II] (see also the hypotheses for this table at the bottom of page 58 of [7]). However, since $p \neq 3$, using [26, Proposition 2.4], we find that rational elliptic curves with a point of order 3 cannot have reduction of Kodaira type I_0^* , II, or I_8^* modulo p . This implies that E^d/\mathbb{Q} cannot have a \mathbb{Q} -rational point of order 3, which is a contradiction. This proves our theorem. \square

Example 3.4. This example shows that the assumption that $p \neq 3$ in Part (ii) of Theorem 3.3 is necessary, and cannot be removed. Consider the elliptic curve E/\mathbb{Q} given by the following Weierstrass equation

$$y^2 + xy + y = x^3 + 549x + 2202.$$

This is the curve with LMFDB [18] label 50a4 (Cremona [9] label 50a4). It has bad reduction modulo 2 and modulo 5, and good reduction modulo every other prime. Using the LMFDB database, we find that, on the one hand, $E(\mathbb{Q})_{\text{tors}}$ is trivial, while, on the other hand, $E_{\mathbb{Q}(\sqrt{-3})}(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z}$.

Let E/\mathbb{Q} be an elliptic curve of conductor N . Work of Breuil, Conrad, Diamond, Taylor, and Wiles (see [3, 36] and [38]) tells us that there exists a modular parametrization $\phi : X_0(N) \rightarrow E$ defined over \mathbb{Q} , where $X_0(N)/\mathbb{Q}$ is the modular curve associated to $\Gamma_0(N)$. Let L/\mathbb{Q} be an imaginary quadratic field satisfying the Heegner hypothesis for E/\mathbb{Q} , that is, all primes that divide the conductor N of E/\mathbb{Q} split in L . Let \mathcal{O}_L be the ring of integers of L . The Heegner hypothesis implies that

there exists an integral ideal \mathcal{N} of \mathcal{O}_L such that $\mathcal{O}_L/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Let $x_1 \in X_0(N)(\mathbb{C})$ be the point corresponding to the isogeny $\mathbb{C}/\mathcal{O}_L \rightarrow \mathbb{C}/\mathcal{N}^{-1}$ (whose kernel is $\mathcal{N}^{-1}/\mathcal{O}_K \cong \mathcal{O}_L/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$). The theory of complex multiplication tells us that $x_1 \in X_0(N)(H)$, where H is the Hilbert class field of L . Finally, let $P_L = \text{Trace}_{H/L}(\phi(x_1))$, which is called the Heegner point associated with L and is well defined up to sign and torsion.

Let m be the Manin constant of E/\mathbb{Q} , let $c(E/\mathbb{Q})$ be the product of the Tamagawa numbers of E/\mathbb{Q} , and let $2u_L$ be the number of roots of unity in L . The following conjecture is due to Gross and Zagier.

Conjecture 3.5 ([13, Conjecture (2.2) in Section V]). *If P_L has infinite order in $E_L(L)$, then P_L generates a subgroup of finite index in $E_L(L)$ and this index equals $c(E/\mathbb{Q}) \cdot m \cdot u_L \cdot \sqrt{|\text{III}(E_L/L)|}$.*

Since the index of P_L in $E_L(L)$ is divisible by $|E(\mathbb{Q})_{\text{tors}}|$, Conjecture 3.5 implies the following weaker conjecture.

Conjecture 3.6 ([13, Conjecture (2.3) in Section V]). *If P_L has infinite order in $E_L(L)$, then $|E(\mathbb{Q})_{\text{tors}}|$ divides $m \cdot c(E/\mathbb{Q}) \cdot u_L \cdot \sqrt{|\text{III}(E_L/L)|}$.*

Very recently Byeon, Yhee, and Kim (see [4] and [5]) have proved the following theorem, which settles Conjecture 3.6 up to a power of 2.

Theorem 3.7. *If E/\mathbb{Q} is an elliptic curve with $E(\mathbb{Q})_{\text{tors}} \not\cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$, then Conjecture 3.6 is true.*

We end this section with the following corollary.

Corollary 3.8. *Let E/\mathbb{Q} be an elliptic curve and $L \neq \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field satisfying the Heegner hypothesis for E/\mathbb{Q} . Assume that the Heegner point P_L has infinite order in $E_L(L)$. Then*

- (i) *The quotient $|E_L(L)_{\text{tors}}|/|E(\mathbb{Q})_{\text{tors}}|$ is equal to a power of 2. In particular, $|E_L(L)_{\text{tors}}|$ divides $m \cdot c(E/\mathbb{Q}) \cdot u_L \cdot \sqrt{|\text{III}(E_L/L)|}$, up to a power of 2.*
- (ii) *If $E(\mathbb{Q})[2] \cong \{0\}$, then $|E_L(L)_{\text{tors}}| = |E(\mathbb{Q})_{\text{tors}}|$. In particular, $|E_L(L)_{\text{tors}}|$ divides $m \cdot c(E/\mathbb{Q}) \cdot u_L \cdot \sqrt{|\text{III}(E_L/L)|}$.*

Proof. Proof of Part (i): We first show that the quotient $|E_L(L)_{\text{tors}}|/|E(\mathbb{Q})_{\text{tors}}|$ is a power of 2. Write $L = \mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$ square-free. Using Part (i) of Theorem 3.3, we find that $E_L(L)_{\text{tors}} \setminus E(\mathbb{Q})_{\text{tors}}$ cannot contain points of order $p > 3$. If $d \neq \pm 3$, then there exists a prime $p \neq 3$ that ramifies in L . Therefore, using Part (i) of Theorem 3.3, we find that $E_L(L)_{\text{tors}} \setminus E(\mathbb{Q})_{\text{tors}}$ cannot contain points of order 3. Since the case $d = 3$ corresponds to a real quadratic field, we have proved that the quotient $|E_L(L)_{\text{tors}}|/|E(\mathbb{Q})_{\text{tors}}|$ is a power of 2. The last assertion of this part follows now immediately from Theorem 3.7.

Proof of Part (ii): If 2 divides $|E_L(L)_{\text{tors}}|$, then it follows from [16, Part (i) of Lemma 1.4] that $E(\mathbb{Q})[2] \not\cong \{0\}$. Therefore, our assumption implies that $|E_L(L)_{\text{tors}}|$ is odd. However, by the previous part, we know that the quotient $|E_L(L)_{\text{tors}}|/|E(\mathbb{Q})_{\text{tors}}|$ is a power of 2. Thus, we have that $|E_L(L)_{\text{tors}}| = |E(\mathbb{Q})_{\text{tors}}|$. Finally, the last assertion follows immediately from Theorem 3.7. This proves our corollary. □

ACKNOWLEDGMENTS

The author was supported by Czech Science Foundation (GAČR) grant 21-00420M and by Charles University Research Center program No. UNCE/SCI/022. I would like to thank Dino Lorenzini for providing some useful comments and suggestions on an earlier version of this manuscript. I would also like to thank two anonymous referees for many valuable comments and suggestions.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

ORCID

Mentzelos Melistas  <https://orcid.org/0000-0002-8468-8943>

REFERENCES

1. P. Deligne, M. Raynaud, D. S. Rim, A. Grothendieck, and M. Raynaud, *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, vol. 288, Springer, Berlin-New York, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim.
2. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer, Berlin, 1990.
3. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over \mathbf{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.
4. D. Byeon, T. Kim, and D. Yhee, *A conjecture of Gross and Zagier: case $E(\mathbf{Q})_{\text{tor}} \cong \mathbb{Z}/3\mathbb{Z}$* , Int. J. Number Theory **15** (2019), no. 9, 1793–1800.
5. D. Byeon, T. Kim, and D. Yhee, *A conjecture of Gross and Zagier: case $E(\mathbf{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$* , Int. J. Number Theory **16** (2020), no. 7, 1567–1572.
6. P. L. Clark and X. Xarles, *Local bounds for torsion points on abelian varieties*, Canad. J. Math. **60** (2008), no. 3, 532–555.
7. S. Comalada, *Twists and reduction of an elliptic curve*, J. Number Theory **49** (1994), no. 1, 45–62.
8. B. Conrad, *A modern proof of Chevalley's theorem on algebraic groups*, J. Ramanujan Math. Soc. **17** (2002), no. 1, 1–18.
9. J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997.
10. E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **108** (2014), no. 2, 923–934.
11. E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields II*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **110** (2016), no. 1, 121–143.
12. F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), no. 1, 1–23.
13. B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L -series*, Invent. Math. **84** (1986), no. 2, 225–320.
14. S. Kamienny, *Torsion points on elliptic curves and q -coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.
15. M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
16. M. Laska and M. Lorenz, *Rational points on elliptic curves over \mathbf{Q} in elementary abelian 2-extensions of \mathbf{Q}* , J. Reine Angew. Math. **355** (1985), 163–172.
17. C. Liedtke and S. Schröer, *The Néron model over the Igusa curves*, J. Number Theory **130** (2010), no. 10, 2157–2197.

18. The LMFDB Collaboration, The L-functions and modular forms database, <http://www.lmfdb.org>, 2019. [Online; accessed 13 March 2023].
19. D. Lorenzini, *Torsion and exceptional units*, Preprint.
20. D. Lorenzini, *Néron models*, Eur. J. Math. **3** (2017), no. 2, 171–198.
21. MathOverflow, Torsion subgroups in families of twists of elliptic curves, <https://mathoverflow.net/questions/76413/torsion-subgroups-in-families-of-twists-of-elliptic-curves>. [Online; accessed 13 March 2023].
22. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **1977** (1978), no. 47, 33–186. With an appendix by Mazur and M. Rapoport.
23. B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612.
24. B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert’s tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575.
25. B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, J. Algebra **314** (2007), no. 1, 419–438.
26. M. Melistas, *On a conjecture of Agashe*, Trans. Amer. Math. Soc. **374** (2021), no. 10, 7143–7160.
27. M. Melistas, *Purely additive reduction of abelian varieties with torsion*, J. Number Theory **239** (2022). <https://doi.org/10.1016/j.jnt.2021.10.015>
28. L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1–3, 437–449.
29. J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.
30. F. Najman, *The number of twists with large torsion of an elliptic curve*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **109** (2015), no. 2, 535–547.
31. J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
32. J. P. Serre, *Galois cohomology*, Springer Monographs in Mathematics. Springer, Berlin, English edition, 2002. Translated from the French by Patrick Ion and revised by the author.
33. J. P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.
34. A. Silverberg, *Applications to cryptography of twisting commutative algebraic groups*, Discrete Appl. Math. **156** (2008), no. 16, 3122–3138.
35. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 2nd ed., vol. 106, Springer, Dordrecht, 2009.
36. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.
37. The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. <https://www.sagemath.org>.
38. A. Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.
39. J. H. Silverman, *Lower bounds for height functions*. Duke Math. J., **51** (1984), no. 2. <https://doi.org/10.1215/s0012-7094-84-05118-4>