GEOMETRICALLY SIMPLE COUNTEREXAMPLES TO A LOCAL-GLOBAL PRINCIPLE FOR QUADRATIC TWISTS

EMILIANO AMBROSI, NIRVANA COPPOLA, AND FRANCESC FITÉ

Abstract. Two abelian varieties A and B over a number field K are said to be strongly locally quadratic twists if they are quadratic twists at every completion of K. While it was known that this does not imply that A and B are quadratic twists over K, the only known counterexamples (necessarily of dimension ≥ 4) are not geometrically simple. We show that, for every prime $p \equiv 13 \pmod{24}$, there exists a pair of geometrically simple abelian varieties of dimension $p-1$ over $\mathbb{Q}$ that are strongly locally quadratic twists but not quadratic twists. The proof is based on Galois cohomology computations and class field theory.

Contents

1. Introduction

1.1. **Twists and local twists.** Let K be a number field, write Γ_K for its absolute Galois group, denote by Σ_K the set of finite places of K, and for $v \in \Sigma_K$ write K_v for the corresponding completion and $K(v)$ for the residue field. If $n \in \mathbb{N}$, we denote with ζ_n a primitive n^{th}-root of unity.

Let A and B be abelian varieties defined over a number field K. A celebrated theorem of Faltings [Fal83] shows that if the reductions of A and B are isogenous over $K(v)$ for a density one set of $v \in \Sigma_K$, then A and B are isogenous over K.

Various variants of this result have been then studied (see e.g. [CT22, Fit24, FP23, KL20, Raj98, Ram00]). In particular, one can show that if the reductions of A and B are isogenous over $\overline{K(v)}$ for a density one set of $v \in \Sigma_K$, then A and B are isogenous over $\overline{K}$ (see for example [KL20, CT22]).

We will work in the category of abelian varieties up to isogeny. In particular, we will say that A and B are *twists* if there exists a finite Galois extension F of K such that the base changes A_F and B_F are isogenous. The result in the previous paragraph naturally raises the question of whether the nature of a twist of A is determined by that of a density one set of its reductions. Different incarnations of this problem have been studied (e.g. [Fit24, FP23]). In this paper we continue this study, focusing on the situation of quadratic twists.

1.2. **Quadratic twists and locally quadratic twists.** To be more precise, recall that the set of twists of A is in a canonical bijection with the Galois cohomology group $H^1(\Gamma_K, \mathrm{Aut}(A_{\overline{K}}))$, where Γ_K is the absolute Galois group of K. For $\alpha \in H^1(\Gamma_K, \mathrm{Aut}(A_{\overline{K}}))$, write A_α for the corresponding twist of A. We say that A_α is a *quadratic twist* of A if α is in the image of $H^1(\Gamma_K, \{\pm 1\}) \to H^1(\Gamma_K, \mathrm{Aut}(A_{\overline{K}}))$, i.e. if α is the image of a continuous character $\chi : \Gamma_K \to \{\pm 1\}$.

We say that A and B are *locally quadratic twists* if their reductions are quadratic twists over $K(v)$ for a density one set of $v \in \Sigma_K$. So, in the spirit of the results of [KL20, CT22], one would like an answer to the following question:

Question 1.1. *If A and B are locally quadratic twists, are they quadratic twists?*

If $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$, the above question admits a positive answer (see [Fit24]). While it is known that the answer is negative in general (see Section 1.3 for more details), only non geometrically simple counterexamples (of dimensions 4 and 6) were known prior to the present work (see [Fit24, Rem. 4.10, §6.2]). The main result of this paper is a strong negative answer to Question 1.1 for geometrically simple abelian varieties of arbitrarily big dimension.

Theorem 1.2. *Fix a prime $p \equiv 13 \pmod{24}$. Every geometrically simple abelian variety of dimension $p-1$ over $\mathbb{Q}$ such that $A_{\overline{\mathbb{Q}}}$ has complex multiplication by $\mathbb{Q}(\zeta_{3p})$ has a twist which is locally quadratic but not quadratic.*

Such abelian varieties exist by [GGL24, Theorem 3.0.1].

1.3. **The Grunwald-Wang counterexample.** Question 1.1 has already been studied by the third named author in [Fit24]. There, it is proven that it has a positive answer if $\dim(A) \leq 3$, and a counterexample is given in dimension 4. To motivate the strategy for the proof of Theorem 1.2, let us recall this counterexample. It consists of the pair of abelian fourfolds A and B, which are the Jacobians of the genus 4 curves over $\mathbb{Q}$ given by the affine models

$$C : y^2 = x^9 + x, \qquad C' : y^2 = x^9 + 16x.$$

The curves C and C' were found via a computer search. The proof given in [Fit24] that A and B are locally quadratic twists involved the explicit computation of the Weil polynomials of A and B via Jacobi sums. The proof that they are not quadratic twists combined the fact that the minimal extension over which all homomorphisms between A and B are defined is $\mathbb{Q}(\zeta_{16}, \sqrt[8]{16})$ with the fact that A and B are not quadratic twists over any of the three quadratic subfields of this extension. This required the computation of Frobenius traces at prescribed primes.

As pointed out to us by Alex Smith, the Grunwald–Wang theorem [AT68, Chap. X] suggests a more conceptual proof: on the one hand, using that 16 admits an 8^{th}-root α_p modulo every odd prime p, one can build the isomorphism $\phi_{\alpha_p} : (x, y) \mapsto (\alpha_p x, \alpha_p^{9/2} y)$ over $\overline{\mathbb{F}}_p$ between the reductions of C and C', showing that A and B are quadratic twists modulo every odd prime; on the other hand, exploiting the fact that 16 does not admit an 8^{th}-root in $\mathbb{Q}$, one can show that A and B are not quadratic twists as explained in Section 4.2.

As mentioned before, we remark that A and B are not geometrically simple. This can be shown by observing that they have potential complex multiplication by $\mathbb{Q}(\zeta_{16})$ but non-primitive CM type.

1.4. **Strongly locally quadratic twists.** We observe that, by Hensel's lemma, 16 has an 8^{th}-root β_p not only over $\mathbb{F}_p$, but also over $\mathbb{Q}_p$, for every odd prime p. Hence A and B have the stronger property of being quadratic twists over $\mathbb{Q}_p$ for all odd p.[1] This leads to the following definition.

Definition 1.3. Let A and B be two abelian varieties over K. We say that A and B are strongly locally quadratic twists if they are quadratic twists over K_v for a density one set of places v of K.

Clearly, if A and B are strongly locally quadratic twists, then they are locally quadratic twists, but we do not know if the converse holds. With this definition, we can state the following stronger version of Theorem 1.2.

Theorem 1.4. *Fix a prime $p \equiv 13 \pmod{24}$. Every geometrically simple abelian variety over $\mathbb{Q}$ of dimension $p-1$ such that $A_{\overline{\mathbb{Q}}}$ has complex multiplication by $\mathbb{Q}(\zeta_{3p})$ has a twist which is strongly locally quadratic but not quadratic.*

We also show (Proposition 3.4) that $n = 39$ is the minimal odd n for which there exists a pair of abelian varieties over $\mathbb{Q}$ with potential complex multiplication by $\mathbb{Q}(\zeta_n)$ which are strongly locally quadratic twists but not quadratic twists. Similar techniques can be used to show that a geometrically simple abelian variety over $\mathbb{Q}$ with potential complex multiplication by $\mathbb{Q}(\zeta_{20})$ could be twisted in order to obtain a counterexample in dimension 4, but we do not know if such abelian varieties exist. Note that our source [GGL24, Theorem 3.0.1] of geometrically simple abelian varieties over $\mathbb{Q}$ with potential complex complex multiplication by $\mathbb{Q}(\zeta_n)$ requires n odd or $n \equiv 2 \pmod{4}$.

1.5. **Final remark.** We would like to end this introduction by stressing the importance of shifting from the notion of locally quadratic twist to that of strongly locally quadratic twist. Let us write $\mathrm{Aut}(A_{\overline{K}})$ to denote $(\mathrm{End}(A_{\overline{K}}) \otimes \mathbb{Q})^\times$. While group representation techniques are well suited for the study of locally quadratic twists, the cohomological approach faces the difficulties of the composition of maps

$$H^1(\Gamma_K, \mathrm{Aut}(A_{\overline{K}})) \to H^1(\Gamma_{K_v}, \mathrm{Aut}(A_{\overline{K}})) \to H^1(\Gamma_{K(v)}, \mathrm{Aut}(A_{\overline{K(v)}})).$$

[1] One can also show that such A and B are quadratic twists over the completion at every place of $\mathbb{Q}(\sqrt{7})$, see Example 4.4

In contrast, since $\mathrm{Aut}(A_{\overline{K}}) \simeq \mathrm{Aut}(A_{\overline{K}_v})$, the study of strongly locally quadratic twists reduces to the study of the first and more accessible of the above composition of maps. The adequacy of the cohomological tools for the study and explicit computation of this map is what ultimately allowed the construction of the counterexamples presented in this article.

Acknowledgements. Fité thanks Université de Strasbourg for its warm hospitality during visits in May 2022, May 2023, and June 2024. Fité was financially supported by the Ramón y Cajal fellowship RYC-2019-027378-I, by the María de Maeztu Program CEX2020-001084-M, and by the AEI grant PID2022-137605NB-I00. Coppola was supported by the ANR-CYCLADES project at Université de Strasbourg. Coppola is a member of the INdAM group GNSAGA. Thanks to Jordan Ellenberg, Alex Smith, and Marco Streng for fruitful conversations.

2. Cohomological characterisation of strongly locally quadratic twists

The main result of this section is Proposition 2.1, that translates the study and the construction of strongly locally quadratic twists to a purely cohomological statement.

2.1. Statements.

Let K be a number field and let A/K be a geometrically simple abelian variety whose geometric endomorphism algebra $\mathrm{End}(A_{\overline{K}}) \otimes \mathbb{Q}$ is a number field E. In this section we give a cohomological characterisation (Proposition 2.1) of the existence of twists of A which are strongly locally quadratic but not (globally) quadratic. Write $K \subseteq L$ for the minimal extension over which all the endomorphisms of A are defined. It is a finite and Galois extension. Let G be the Galois group of L/K and consider the following commutative diagram with exact rows and columns.

$$\begin{array}{ccccccc} & & & & H^1(\Gamma_K, \{\pm1\}) & & \\ & & & & \downarrow & & \\ & & & & H^1(\Gamma_K, E^\times) & & \\ & & & & \downarrow & & \\ 1 & \longrightarrow & H^1(G, E^\times/\{\pm1\}) & \longrightarrow & H^1(\Gamma_K, E^\times/\{\pm1\}) & \longrightarrow & H^1(\Gamma_L, E^\times/\{\pm1\}) \\ & & & & \downarrow{\scriptstyle \delta} & & \\ & & & & H^2(\Gamma_K, \{\pm1\}) & & \end{array}$$

The vertical sequence is induced by the exact sequence of G-modules

$$1 \to \{\pm1\} \to E^\times \to E^\times/\{\pm1\} \to 1$$

and the horizontal one by inflation and restriction. For an element $x \in H^1(G, E^\times/\{\pm1\})$ consider the following conditions:

(i) $x \neq 1$;
(ii) x restricts to 1 in $H^1(C, E^\times/\{\pm1\})$ for every cyclic subgroup $C \subseteq G$;
(iii) x maps to 1 in $H^2(\Gamma_K, \{\pm1\})$.

Proposition 2.1. *The following are equivalent:*

(1) there exists a twist B of A which is strongly locally quadratic but not quadratic;

(2) *there exists an element* $x \in H^1(G, E^\times/\{\pm 1\})$ *satisfying* $(i) - (ii) - (iii)$ *above.*

Corollary 2.2. *If G is cyclic then every strongly locally quadratic twist is quadratic.*

We will also need a straightforward variant of Proposition 2.1. We say that a subgroup $C \subseteq G$ is *maximally cyclic* if it is cyclic and every subgroup $H \subseteq G$ that properly contains C is not cyclic. Since condition (ii) is clearly equivalent to:

(ii') x restricts to 1 in $H^1(C, E^\times/\{\pm 1\})$ for every maximally cyclic subgroup $C \subseteq G$,

we can restate Proposition 2.1 as follows.

Proposition 2.3. *The following are equivalent:*

(1) *there exists a twist B of A which is strongly locally quadratic but not quadratic;*
(2) *there exists an element* $x \in H^1(G, E^\times/\{\pm 1\})$ *satisfying* $(i) - (ii') - (iii)$ *above.*

Before giving the proof of Proposition 2.1, we state a general lemma that will be useful in the rest of the paper.

Lemma 2.4. *If* $K = L$*, then every strongly locally quadratic twist of A is a quadratic twist.*

Proof. Since all endomorphisms of A are defined over K, we also have that all the endomorphisms of A are defined over K_v for every $v \in \Sigma_K$. Hence

$$H^1(\Gamma_K, E^\times) = \mathrm{Hom}(\Gamma_K, E^\times) \quad \text{and} \quad H^1(\Gamma_{K_v}, E^\times) = \mathrm{Hom}(\Gamma_{K_v}, E^\times),$$

and the maps

$$H^1(\Gamma_K, \{\pm 1\}) \to H^1(\Gamma_K, E^\times) \quad \text{and} \quad H^1(\Gamma_{K_v}, \{\pm 1\}) \to H^1(\Gamma_{K_v}, E^\times)$$

are injective. Let B be a strongly locally quadratic twist of A corresponding to an element $\chi \in H^1(\Gamma_K, E^\times)$. It is enough to show that $\mathrm{Im}(\chi) = \{\pm 1\}$. But this holds on every decomposition group by assumption, hence it holds on all of Γ_K, since decomposition groups form a dense subset of Γ_K. □

2.2. **Proof.** We now prove Proposition 2.1. We start by proving that (1) implies (2). Let $\tilde{x} \in H^1(\Gamma_K, E^\times)$ be the cohomology class associated to B and let x be its image in $H^1(\Gamma_K, E^\times/\{\pm 1\})$. By construction, $\delta(x) = 1$ and, since B is not a quadratic twist of A, we have that $x \neq 1$. Since A and B are locally quadratic twists, by Lemma 2.4, they are quadratic twists over L, hence the restriction of x in $H^1(\Gamma_L, E^\times/\{\pm 1\})$ is trivial, and thus $x \in H^1(G, E^\times/\{\pm 1\})$. We are left to show that x is trivial when restricted to any cyclic subgroup $C \subseteq G$. By Chebotarev, for every cyclic subgroup $C \subseteq G$ there is a positive density set of finite places v of K (unramified in L) such that the decomposition group D_v is C. In particular we can choose one v such that A_v and B_v are quadratic twists over K_v, so the restriction of x to $H^1(\Gamma_{K_v}, E^\times/\{\pm 1\})$ is trivial. The conclusion follows from the commutative diagram

$$\begin{array}{ccc} H^1(G, E^\times/\{\pm 1\}) & \hookrightarrow & H^1(\Gamma_K, E^\times/\{\pm 1\}) \\ \downarrow & & \downarrow \\ H^1(D_v, E^\times/\{\pm 1\}) & \hookrightarrow & H^1(\Gamma_{K_v}, E^\times/\{\pm 1\}), \end{array} \tag{2.1}$$

since the bottom horizontal arrow is injective.

We now prove prove that (2) implies (1). Let x be as in the statement. Since the top horizontal map of (2.1) is injective, the image of x in $H^1(\Gamma_K, E^\times/\{\pm 1\})$, that we still denote by x, is nontrivial. By assumption (iii), one has $\delta(x) = 1$ (where δ is the connecting homomorphism defined in Section 2.1), so x lifts to an element $\tilde{x}$ in $H^1(\Gamma_K, E^\times)$. Thus $\tilde{x}$ defines a twist $A_{\tilde{x}}$ of A, which is not quadratic since $x \neq 1$. Let Σ be the set of finite places of K which are not ramified in L, so that, for every $v \in \Sigma$, the decomposition group D_v is cyclic. Since Σ consists of all but finitely many places of K, it is enough to show that for every $v \in \Sigma$, the twist $A_{\tilde{x},v}$ of A_v is quadratic. For this, it is enough to show that the restriction of $x \in H^1(\Gamma_K, E^\times/\{\pm 1\})$ to $H^1(\Gamma_{K_v}, E^\times/\{\pm 1\})$ is trivial. Since D_v is cyclic, this follows from assumption (ii) and the commutative diagram (2.1).

3. Geometrically simple counterexamples

In this section, after some group cohomology preliminaries, we prove Theorem 1.4. We then discuss the minimality of our counterexample for $n = 39$ among abelian varieties with potential complex multiplication by $\mathbb{Q}(\zeta_n)$ for odd n.

3.1. Preliminaries.

3.1.1. *Cohomology of cyclic groups.* Let C be a finite cyclic group of cardinality n acting on an abelian group M, written multiplicatively, and write $g \in C$ for a generator. Let $M^C \subseteq M$ be the group of elements that are fixed by C and $\mathcal{N}_C : M \to M$ be the norm map, sending $m \in M$ to $mg(m) \dots g^{n-1}(m)$. Recall from [Ser89, VIII, §4] that one has natural identifications:

$$H^i(C; M) = \begin{cases} M^C & \text{if } i = 0, \\ \mathrm{Ker}(\mathcal{N}_C)/\langle g(m)m^{-1}\rangle_{m \in M} & \text{if } i \text{ is odd}, \\ M^C/\mathrm{Im}(\mathcal{N}_C) & \text{if } i \text{ is even}. \end{cases} \tag{3.1}$$

Under these identifications, if

$$1 \to N \to M \to Q \to 1$$

is an exact sequence of C-abelian groups, then the connecting morphism

$$\delta : \mathrm{Ker}(\mathcal{N}_C)/\langle g(q)q^{-1}\rangle_{q \in Q} \simeq H^1(C, Q) \to H^2(C, N) \simeq N^C/\mathrm{Im}(\mathcal{N}_C)$$

has the following description: for $x \in \mathrm{Ker}(\mathcal{N}_C)$, choose a lift $\widetilde{x} \in M$ and set $\delta(x) := \mathcal{N}_C(\widetilde{x})$.

Finally, for $i > 0$ we note that $H^i(C, \{\pm 1\}) \simeq \{\pm 1\}$ if C is of even order and $H^i(C, \{\pm 1\}) = 1$ otherwise.

3.1.2. *Preliminary lemmas.* Assume that E/F is a finite Galois extension of number fields with Galois group G and consider the short exact sequence of G-modules

$$1 \to \{\pm 1\} \to E^\times \to E^\times/\{\pm 1\} \to 1. \tag{3.2}$$

Lemma 3.1.
1. *The connective morphism $H^1(G, E^\times/\{\pm 1\}) \to H^2(G, \{\pm 1\})$ is injective. If G is cyclic, it is induced by the norm map under the identifications (3.1).*
2. *There is a natural short exact sequence*

$$1 \to F^\times/\{\pm 1\} \to (E^\times/\{\pm 1\})^G \to H^1(G, \{\pm 1\}) \to 1.$$

Proof.
1. Injectivity follows from Hilbert's 90th theorem, while the description of the map in the case of a cyclic group follows from the previous discussion.
2. This follows again from Hilbert's 90th theorem applied to the exact sequence in cohomology induced by (3.2). □

Assume now that K is a number field and that A is a geometrically simple abelian variety over K whose geometric endomorphism algebra $\mathrm{End}(A_{\overline{K}}) \otimes \mathbb{Q}$ is a number field E. We let $K \subseteq L$ be the minimal extension over which all the endomorphisms of A are defined. By Galois theory, $\mathrm{Gal}(L/K)$ is isomorphic to $\mathrm{Gal}(E/F)$, where $F = \mathrm{End}(A) \otimes \mathbb{Q}$.

Lemma 3.2. *Let $K \subseteq F \subseteq L$ be an intermediate Galois extension corresponding to a normal subgroup $H \subseteq G = \mathrm{Gal}(L/K)$. Let $x \in H^1(G, E^\times)$ and suppose that $[F : K]$ is odd. Then x satisfies the conditions $(i), (ii), (iii)$ of Proposition 2.1 if and only its restriction to H does.*

Proof. Consider the commutative diagram

$$\begin{array}{ccc} H^1(G, E^\times/\{\pm 1\}) & \hookrightarrow & H^2(\Gamma_K, \{\pm 1\}) \\ \downarrow & & \downarrow \\ H^1(H, E^\times/\{\pm 1\}) & \hookrightarrow & H^2(\Gamma_F, \{\pm 1\}). \end{array}$$

Since $[G : H]$ is odd, by [NSW00, Prop. 1.6.9] the rightmost vertical map is injective, so conditions (i) and (iii) are equivalent for H and G.

To prove that also condition (ii) is equivalent for H and G, observe first that condition (ii) for G clearly implies the one for H. Conversely, assume now that condition (ii) holds for H, and let $C \subseteq G$ be a cyclic subgroup. Consider the commutative diagram

$$\begin{array}{ccccc} H^1(G, E^\times/\{\pm 1\}) & \longrightarrow & H^1(C, E^\times/\{\pm 1\}) & \hookrightarrow & H^2(C, \{\pm 1\}) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(H, E^\times/\{\pm 1\}) & \longrightarrow & H^1(C \cap H, E^\times/\{\pm 1\}) & \hookrightarrow & H^2(C \cap H, \{\pm 1\}) \end{array}$$

where the injectivity of the rightmost horizontal arrows is due to Lemma 3.1. Since $C/C \cap H \simeq CH/H \subseteq G/H$ is of odd order, the rightmost vertical map is also injective, thus the vanishing of the restriction of x to $H^1(C \cap H, E^\times/\{\pm 1\})$ implies the vanishing of the restriction of x to $H^1(C, E^\times/\{\pm 1\})$. □

3.2. **An infinite family of counterexamples.** We start recalling the statement of our main result.

Theorem 3.3. *Let p be an odd prime such that $p \equiv 13 \pmod{24}$. Let A be a geometrically simple abelian variety over $\mathbb{Q}$ such that $A_{\overline{\mathbb{Q}}}$ has complex multiplication by $E := \mathbb{Q}(\zeta_{3p})$. Then there exists a twist of A which is strongly locally quadratic but not quadratic.*

Since A has potential complex multiplication by E and it is geometrically simple, by [Shi98, Prop. 26 and Prop. 28, Chap. II], the reflex field of E is E itself. Then, by [Shi98, Prop. 20.4] or [Shi71, Prop. 5.17] or [Lan83, Thm. 1.1, Chap. 3], the field E is also the minimal field of definition of all the endomorphisms of A.

We write $G := \mathrm{Gal}(E/\mathbb{Q})$ and $G_1 := \mathrm{Gal}(E/\mathbb{Q}(\sqrt{-3}))$, so that $G/G_1 \simeq \mathbb{Z}/2\mathbb{Z}$. Let σ be the projection of complex conjugation to G/G_1. It naturally acts on $(E^\times/\{\pm 1\})^{G_1}$.

Since $p \equiv 1 \pmod 3$, it splits in $\mathbb{Q}(\sqrt{-3})$. Hence there exist $a, b \in \mathbb{Q}$ such that $a^2 + 3b^2 = 3p$.

We let $y := \dfrac{a + b\sqrt{-3}}{\sqrt{-3p}} \in E^\times/\{\pm 1\}$ and we observe that $y \in (E^\times/\{\pm 1\})^{G_1}$. By construction, one has $\sigma(y)y = -1$, so we can associate to y a cohomology class $x \in H^1(G/G_1, (E^\times/\{\pm 1\})^{G_1})$. By inflation, we get a cohomology class $x \in H^1(G, E^\times/\{\pm 1\})$. By Proposition 2.1, it is then enough to show that x satisfies the conditions (i), (ii') and (iii) from Section 2.1.

3.2.1. *Condition (i).* Since the inflation map is injective, it is enough to show that x is nontrivial in $H^1(G/G_1, (E^\times/\{\pm 1\})^{G_1})$. By Lemma 3.1, there is a short exact sequence of G/G_1-modules

$$1 \to \mathbb{Q}(\sqrt{-3})^\times/\{\pm 1\} \to (E^\times/\{\pm 1\})^{G_1} \to H^1(G_1, \{\pm 1\}) \to 1.$$

Since G_1 is cyclic of even order, we have that $H^1(G_1, \{\pm 1\}) \simeq \{\pm 1\}$. Since $y \in (E^\times/\{\pm 1\})^{G_1}$ is not in the image of $\mathbb{Q}(\sqrt{-3})^\times/\{\pm 1\} \to (E^\times/\{\pm 1\})^{G_1}$, it maps nontrivially in $H^1(G_1, \{\pm 1\})$. Since G/G_1 is cyclic of even order and it acts trivially on $H^1(G_1, \{\pm 1\}) \simeq \{\pm 1\}$, one has

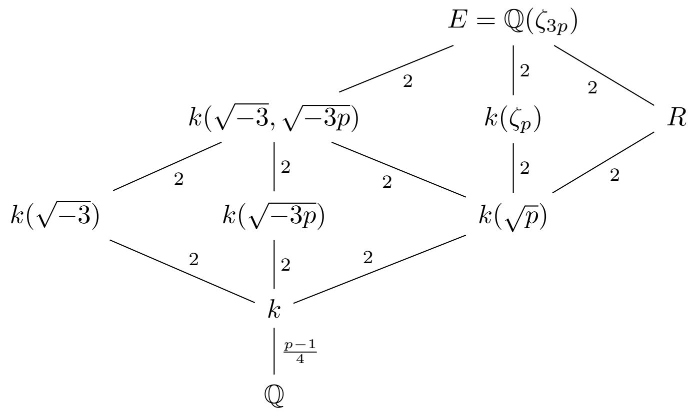
$$H^1(G/G_1, H^1(G_1, \{\pm 1\})) \simeq H^1(G/G_1, \{\pm 1\}) \simeq \{\pm 1\} \simeq H^1(G_1, \{\pm 1\}).$$

The composition of the map

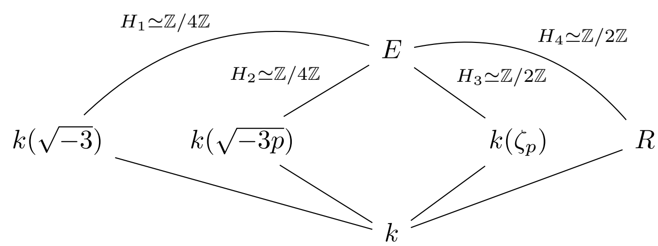
$$H^1(G/G_1, (E^\times/\{\pm 1\})^{G_1}) \to H^1(G/G_1, H^1(G_1, \{\pm 1\}))$$

with the above isomorphism sends x to the image of y under the map $(E^\times/\{\pm 1\})^{G_1} \to H^1(G_1, \{\pm 1\})$. We have seen that this image is nontrivial, and hence x is nontrivial as well.

3.2.2. *Condition (ii').* Let $\mathbb{Q} \subseteq k$ be the maximal subextension of $\mathbb{Q} \subseteq E$ of odd degree. By Lemma 3.2, proving (ii') is equivalent to proving it after restricting to k. We will denote by R the maximal totally real subfield $k(\zeta_{3p} + \overline{\zeta_{3p}})$ of E. Since $p \not\equiv 1 \pmod 8$, the group $H := \mathrm{Gal}(E/k)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and we have the following diagram of intermediate extensions.



There are only four maximally cyclic subgroups $H_1, \dots, H_4 \subseteq H$, corresponding to the four extensions of k depicted in the diagram below.



We write σ_i for a generator of H_i. Since, by construction, x is inflated from H/H_1, it goes to 1 in $H^1(H_1, E^\times/\{\pm 1\})$.

Recall from Lemma 3.1 that the norm map

$$\mathcal{N}_{H_i} : H^1(H_i, E^\times/\{\pm 1\}) \to H^2(H_i, \{\pm 1\}) \simeq \{\pm 1\}$$

is injective. Hence it will suffice to show that $\mathcal{N}_{H_i}(y) = 1$ for $i = 2, 3, 4$.

Since H_2 fixes $k(\sqrt{-3p})$, one has $\sigma_2(y) = \dfrac{a - b\sqrt{-3}}{\sqrt{-3p}}$. In particular, we have

$$\mathcal{N}_{H_2}(y) = \prod_{i=0}^{3} \sigma_2^i(y) = (y\sigma(y))^2 = \left(\frac{3p}{-3p}\right)^2 = 1.$$

Foror $i = 3, 4$, we see that σ_i acts nontrivially on both $\sqrt{-3}$ and $\sqrt{-3p}$, thus sending y to its complex conjugate. Therefore $\mathcal{N}_{H_i}(y) = y\sigma_i(y) = 1$.

3.2.3. *Condition (iii).* Recall that, for every field M, we have $H^2(\Gamma_M, \{\pm 1\}) \simeq \mathrm{Br}(M)[2]$. Hence, the fundamental exact sequence of class field theory yields a short exact sequence

$$1 \to H^2(\Gamma_{\mathbb{Q}}, \{\pm 1\}) \to H^2(\Gamma_{\mathbb{R}}, \{\pm 1\}) \times \prod_{q \in \Sigma_{\mathbb{Q}}} H^2(\Gamma_{\mathbb{Q}_q}, \{\pm 1\}) \xrightarrow{\sum \mathrm{res}_q} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \to 0,$$

where $\mathrm{res}_\infty : H^2(\Gamma_{\mathbb{R}}, \{\pm 1\}) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and $\mathrm{res}_q : H^2(\Gamma_{\mathbb{Q}_q}, \{\pm 1\}) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ are the residue morphisms. Hence, it is enough to show that the class of x becomes trivial in $H^2(\Gamma_{\mathbb{R}}, \{\pm 1\})$ and in $H^2(\Gamma_{\mathbb{Q}_q}, \{\pm 1\})$ for all primes q, except at most one.

To check the infinite place, write $C := \mathrm{Gal}(E/R)$ for the Galois group of the maximal totally real subfield $R \subseteq E$. Since C is cyclic, the restriction of x to $H^1(C, E^\times/\{\pm 1\})$ is trivial by Section 3.2.2. Then the commutative diagram

$$\begin{array}{ccccc} H^1(G, E^\times/\{\pm 1\}) & \longrightarrow & H^1(\Gamma_{\mathbb{Q}}, E^\times/\{\pm 1\}) & \longrightarrow & H^2(\Gamma_{\mathbb{Q}}, \{\pm 1\}) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(C, E^\times/\{\pm 1\}) & \longrightarrow & H^1(\Gamma_{\mathbb{R}}, E^\times/\{\pm 1\}) & \longrightarrow & H^2(\Gamma_{\mathbb{R}}, \{\pm 1\}) \end{array}$$

shows that the image of x in $H^2(\Gamma_{\mathbb{R}}, \{\pm 1\})$ is trivial.

We claim that, for all primes $q \neq 3$, the decomposition group $D_q \subseteq G$ is cyclic. If $q \neq p$, this follows from the fact that q is unramified in E. To check that also D_p is cyclic, we first observe that

$$\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1,$$

by quadratic reciprocity and the assumption $p \equiv 1 \pmod 4$. Hence p splits in $\mathbb{Q}(\sqrt{-3})$, so that $D_p \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ is cyclic.

In particular, the restriction of x to $H^1(D_q, E^\times/\{\pm 1\})$ vanishes by Section 3.2.2. Hence the commutative diagram

$$\begin{array}{ccccc} H^1(G, E^\times/\{\pm 1\}) & \longrightarrow & H^1(\Gamma_{\mathbb{Q}}, E^\times/\{\pm 1\}) & \longrightarrow & H^2(\Gamma_{\mathbb{Q}}, \{\pm 1\}) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(D_q, E^\times/\{\pm 1\}) & \longrightarrow & H^1(\Gamma_{\mathbb{Q}_q}, E^\times/\{\pm 1\}) & \longrightarrow & H^2(\Gamma_{\mathbb{Q}_q}, \{\pm 1\}) \end{array}$$

shows that the image of x in $H^2(\Gamma_{\mathbb{Q}_q}, \{\pm 1\})$ is trivial.

3.3. **Minimality of the counterexample.** In the previous section, we constructed an infinite family of geometrically simple counterexamples to Question 1.1. In particular, when $p = 13$, we obtain one example in dimension 12. We now show that such a counterexample is the one of smaller dimension among all geometrically simple abelian varieties with geometric complex multiplication by $\mathbb{Q}(\zeta_n)$ for odd n. To do so, let n be an odd number such that $\phi(n) < 24$ and let A be an abelian variety as above.

If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic (i.e. n is a power of an odd prime), then no twist of A can yield a counterexample by Corollary 2.2. This leaves only three possibilities for n, namely $15 = 3 \cdot 5$, $21 = 3 \cdot 7$ and $33 = 3 \cdot 11$. All of these are excluded by the following proposition.

Proposition 3.4. *Let p be a prime. Let A be an abelian variety over $\mathbb{Q}$ such that $A_{\overline{\mathbb{Q}}}$ has complex multiplication by $E := \mathbb{Q}(\zeta_{3p})$ and is geometrically simple. Assume that either*

(1) $p \equiv 2 \pmod 3$*, or*

(2) $p \equiv 3 \pmod 4$.

Then, every strongly locally quadratic twist of A is a (global) quadratic twist of A.

Proof. Since A is geometrically simple and has potential complex multiplication by E, by [Shi71, Prop. 5.17] or [Lan83, Thm. 1.1, Chap. 3], the field E is also the minimal field of definition of all the endomorphisms of A. Let $G := \mathrm{Gal}(E/\mathbb{Q})$. By Proposition 2.1, it is enough to show that there are no non trivial elements in $H^1(G, E^\times/\{\pm 1\})$ which vanish on every cyclic subgroup. To show this, it suffices to prove that there exists at least one cyclic subgroup $H \subseteq G$ such that $H^1(G/H, (E^\times/\{\pm 1\})^H) = 1$, since then restriction to H is injective by inflation-restriction. For this we will use the following lemma.

Lemma 3.5. *Let $H \subseteq G$ be a cyclic index two subgroup corresponding to an imaginary quadratic field $F = \mathbb{Q}(\sqrt{-d})$ for $d \in \mathbb{Q}^\times$. Then*

(1) $H^1(G/H, F^\times/\{\pm 1\}) = 1$.

(2) Suppose there exists $x \in (E^\times/\{\pm 1\})^H$ such that $\mathcal{N}_{G/H}(x) \notin \mathcal{N}_{G/H}(F^\times)$, then $H^1(G/H, (E^\times/\{\pm 1\})^H) = 1$.

Proof. We first consider part (1). By Hilbert's 90th theorem, the sequence $1 \to \{\pm 1\} \to F^\times \to F^\times/\{\pm 1\} \to 1$ induces a short exact sequence

$$1 \to H^1(G/H, F^\times/\{\pm 1\}) \to H^2(G/H, \{\pm 1\}) \to H^2(G/H, F^\times).$$

Hence, using the identification (3.2), it is enough to show that the natural map

$$\{\pm 1\} \simeq H^2(G/H, \{\pm 1\}) \to H^2(G/H, F^\times) \simeq (F^\times)^{G/H}/\mathcal{N}_{G/H}(F^\times)$$

is injective. This follows from the fact that -1 is not a norm for the imaginary field extension $F/\mathbb{Q}$.

To prove part (2), let us write M to denote the quotient of $E^\times/\{\pm 1\}$ by $F^\times/\{\pm 1\}$. The exact sequence from Lemma 3.1

$$1 \longrightarrow F^\times/\{\pm 1\} \longrightarrow (E^\times/\{\pm 1\})^H \longrightarrow H^1(H, \{\pm 1\}) \longrightarrow 1,$$

shows that M is isomorphic to $H^1(H, \{\pm 1\}) \simeq \{\pm 1\}$, so that that, in particular, $\mathrm{Ker}(\mathcal{N}_{G/H} : M \to M) = M$. The above exact sequence, together with part (1) of the lemma, induces an exact sequence

$$1 \to H^1(G/H, (E^\times/\{\pm 1\})^H) \to H^1(G/H, M) \xrightarrow{\delta} H^2(G/H, F^\times/\{\pm 1\}),$$

and thus it suffices to show that δ is injective. On the one hand, observe that $H^1(G/H, M) \simeq \{\pm 1\}$. On the other hand, by (3.2), if σ is the nontrivial element of G/H, we have

$$H^1(G/H, M) \simeq \mathrm{Ker}(\mathcal{N}_{G/H})/\langle \sigma(m)m^{-1}\rangle_{m\in M} = M/\langle \sigma(m)m^{-1}\rangle_{m\in M}.$$

Using the identifications from (3.2), we may rewrite δ as

$$\mathcal{N}_{G/H} : M/\langle \sigma(m)m^{-1}\rangle_{m\in M} \simeq \{\pm 1\} \to (F^\times)^{G/H}/\mathcal{N}_{G/H}(F^\times).$$

From this, we see that $\delta(-1) = \mathcal{N}_{G/H}(x)$ and the injectivity of δ follows from the hypothesis that $\mathcal{N}_{G/H}(x) \notin \mathcal{N}_{G/H}(F^\times)$.

□

We now come back to the proof of Proposition 3.4. Suppose first that $p \equiv 2 \pmod 3$. Recall that $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$. Let $G_1 \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ be the cyclic subgroup of G fixing $F_1 := \mathbb{Q}(\sqrt{-3})$. We claim that $H^1(G/G_1, (E^\times/\{\pm 1\})^{G_1}) = 1$. By [Was97, Exercise 2.1] one has that either $\sqrt{-p} \in E^\times$ or $\sqrt{-3p} \in E^\times$. Hence, by Lemma 3.5, it is enough to show that either $p = \mathcal{N}_{G/G_1}(\sqrt{-p})$ or $3p = \mathcal{N}_{G/G_1}(\sqrt{-3p})$ is not a norm for the field extension $F_1/\mathbb{Q}$. Since 3 is a norm, this amounts to showing that p is not a norm. The latter follows from the condition $p \equiv 2 \pmod 3$, which is equivalent to the primality of the ideal $p\mathcal{O}_{F_1}$.

Suppose now that $p \equiv 3 \pmod 4$. In this case $\sqrt{-p} \in E^\times$ by [Was97, Exercise 2.1], and the extension $F_2 := \mathbb{Q}(\sqrt{-p}) \subseteq E$ is cyclic. Let G_2 be its cyclic Galois group. We claim that $H^1(G/G_i, (E^\times/\{\pm 1\})^{G_i})$ is trivial for either $i = 1$ or $i = 2$. By Lemma 3.5, it is enough to show that either $3 = \mathcal{N}_{G/G_2}(\sqrt{-3})$ is not a norm in $F_2/\mathbb{Q}$ or that $p = \mathcal{N}_{G/G_1}(\sqrt{-p})$ is not a norm in $F_1/\mathbb{Q}$. This amounts to showing that either

$$\left(\frac{-3}{p}\right) = -1 \qquad \text{or} \qquad \left(\frac{-p}{3}\right) = -1.$$

This is implied by the fact that the product of the above two Legendre symbols is -1, as a consequence of quadratic reciprocity and the assumption $p \equiv 3 \pmod 4$. □

4. Grunwald-Wang style counterexamples

In this section we generalise the Grunwald-Wang counterexample from [Fit24] recalled in Section 1.3. Let K be a field and A be an abelian variety over K. Let $K \subseteq L$ be the minimal extension over which all the endomorphisms of A are defined and let $G := \mathrm{Gal}(L/K)$. Write E for $\mathrm{End}(A_L) \otimes \mathbb{Q}$.

4.1. **Preliminaries.** Let B be an abelian variety over K such that B_L is the quadratic twist of A_L by a quadratic character χ of Γ_L. Let $L \subseteq L_\chi$ be the quadratic extension cut by χ. Since $K \subseteq L_\chi$ is the field over which all the endomorphisms of $A \times B$ are defined, it is a Galois extension of K whose Galois group is a central extension

$$1 \to \{\pm 1\} \to \mathrm{Gal}(L_\chi/K) \to G \to 1. \tag{4.1}$$

Proposition 4.1. *If A and B are quadratic twists then (4.1) splits, so that*

$$\mathrm{Gal}(L_\chi/K) \simeq G \times \{\pm 1\}.$$

Proof. Recall that $H^2(G, \{\pm 1\})$ is in bijection with the set of isomorphisms classes of central extensions of the form $1 \to \{\pm 1\} \to H \to G \to 1$.

Let $\mathrm{Tra} : H^1(\Gamma_L, \{\pm 1\}) \to H^2(G, \{\pm 1\})$ be the transgression map induced by the inclusion of the normal subgroup $\Gamma_L \subseteq \Gamma_K$. Under the aforementioned bijection, the class of $\mathrm{Tra}(\chi)$ identifies with the Galois group of the Galois extension L_χ/K. Hence, it is enough to show that if B is a quadratic twist of A, then $\mathrm{Tra}(\chi) = 1$.

By [NSW00, Proposition 1.6.7], we have a commutative diagram

$$\begin{array}{ccccc} H^1(\Gamma_K, \{\pm 1\}) & \xrightarrow{\mathrm{Res}} & H^1(\Gamma_L, \{\pm 1\})^G & \xrightarrow{\mathrm{Tra}} & H^2(G, \{\pm 1\}) \\ \downarrow \iota & & \downarrow \iota' & & \\ H^1(\Gamma_K, E^\times) & \xrightarrow{\mathrm{Res}} & H^1(\Gamma_L, E^\times)^G & & \end{array}$$

whose first row is exact. Observe that ι' is injective, since the action of Γ_L on $E^\times$ is trivial and then $H^1(\Gamma_K, E^\times)$ identifies with the quotient of $\mathrm{Hom}(\Gamma_K, E^\times)$ modulo conjugation.

Let c_B be the element in $H^1(\Gamma_K, E^\times)$ corresponding to B. Note that $\mathrm{Res}(c_B) = \iota'(\chi)$. If A and B are quadratic twists, then there exists a quadratic character $\tilde{\chi}$ of Γ_K such that $\iota(\tilde{\chi}) = c_B$. But then

$$\iota'(\mathrm{Res}(\tilde{\chi})) = \mathrm{Res}(\iota(\tilde{\chi})) = \mathrm{Res}(c_B) = \iota'(\chi).$$

The injectivity of ι' implies that $\chi = \mathrm{Res}(\tilde{\chi})$ and hence $\mathrm{Tra}(\chi) = \mathrm{Tra}(\mathrm{Res}(\tilde{\chi})) = 1$. □

4.2. **Grunwald-Wang counterexamples.** Let m be a positive integer. Assume that E contains $\mathbb{Q}(\zeta_{2m})$. In the following, we let μ_n denote the set of all n^{th} roots of unity. For $\alpha \in K^\times$, let $[\alpha] \in H^1(\Gamma_K, \mu_{2m}) \simeq K^\times/(K^\times)^{2m}$ the corresponding class. Define A_α as the abelian variety corresponding to the image of $[\alpha]$ through the map $H^1(\Gamma_K, \mu_{2m}) \to H^1(\Gamma_K, E^\times)$.

Example 4.2. Let A be the Jacobian of the curve given by the affine model $C : y^2 = x^{m+1} + x$. The action of μ_{2m} on C given by $(x, y) \mapsto (\zeta_m x, \zeta_{2m} y)$ yields an inclusion of $\mathbb{Q}(\zeta_{2m})$ in E. If C_α denotes the curve given by $y^2 = x^{m+1} + \alpha x$, then

$$\phi_\alpha : C \to C_\alpha\,, \qquad \phi_\alpha(x, y) = (\alpha^{1/m} x, \alpha^{(m+1)/(2m)} y)$$

is an isomorphism over $\overline{K}$. The map $\xi_\alpha : \Gamma_K \to \mu_{2m}$ defined as $\xi_\alpha(s) := \phi_\alpha^{-1} \circ {}^s\phi_\alpha$ is a 1-cocicle. An easy calculation shows that the class of ξ_α corresponds to $[\alpha]$ under the Kummer isomorphism. Hence A_α is the Jacobian of the curve C_α.

Proposition 4.3. *Assume that $L = K(\zeta_{2m})$, that the only roots of unity contained in K are ± 1, and that there exists a finite subset $S \subseteq \Sigma_K$ such that $\alpha \in K_v^{\times, m}$ for all $v \notin S$.*

(1) *The abelian varieties A and A_α are strongly locally quadratic twists. More precisely, A and A_α are quadratic twists over K_v for all $v \notin S$.*
(2) *If A and A_α are quadratic twists then either α or $-\alpha$ is an m^{th} power.*

Proof. Consider the exact sequence

$$1 \to \mu_2 \to \mu_{2m} \xrightarrow{(-)^2} \mu_m \to 1$$

where the first arrow is the natural inclusion. For any field extension $K \subseteq F$, one has an induced short exact sequence in cohomology

$$H^1(\Gamma_F, \mu_2) \to H^1(\Gamma_F, \mu_{2m}) \to H^1(\Gamma_F, \mu_m),$$

which, in turn, identifies with the exact sequence

$$F^\times/(F^\times)^2 \xrightarrow{(-)^m} F^\times/(F^\times)^{2m} \to F^\times/(F^\times)^m$$

where the last arrow is the natural projection. This shows that $[\alpha]_F \in H^1(\Gamma_F, \mu_{2m})$ is in the image of $H^1(\Gamma_F, \mu_2)$ as soon as α is an m^{th}-power in F, since this implies that it becomes trivial in $H^1(\Gamma_F, \mu_m)$. Taking F to be K_v for any $v \notin S$, and considering the commutative diagram

$$\begin{array}{ccc} H^1(\Gamma_F,\mu_2) & \longrightarrow & H^1(\Gamma_F,\mu_{2m}) \\ & \searrow \quad \swarrow & \\ & H^1(\Gamma_F,E^\times), & \end{array}$$

we obtain (1).

We are left to prove that if A and A_α are quadratic twists then either α or $-\alpha$ is an m^{th} power. By the Grunwald-Wang theorem [AT68, p. 96], since $\zeta_{2m} \in L$ and α is locally an m^{th} power, it becomes an m^{th} power in L, so that $L(\sqrt[2m]{\alpha})/L$ is of degree two and A_L and $A_{\alpha,L}$ are quadratic twists by the character defining the extension $L \subseteq L(\sqrt[2m]{\alpha})$.

By Proposition 4.1, we see that

$$\mathrm{Gal}(K(\zeta_{2m}, \sqrt[2m]{\alpha})/K) = \mathrm{Gal}(L(\sqrt[2m]{\alpha})/K) \simeq \mathrm{Gal}(L/K) \times \{\pm 1\}$$

is abelian. Since the only roots of unity contained in K are ± 1, by [Sch77, Theorem 2] we deduce that α^2 is a $2m^{th}$ power, hence that one of α or $-\alpha$ is m^{th} power. This concludes the proof. □

Example 4.4. In Example 4.2 , take $K = \mathbb{Q}(\sqrt{7})$, $m = 4$, and $\alpha = 16$. One has that $L = K(\zeta_{16})$. Then A and A_α are everywhere strongly locally quadratic, but not globally quadratic, since neither 16 or -16 are 8^{th}-powers in K but 16 is an 8^{th}-power in every localization of K (see [AT68, p. 98]). It would be interesting to determine for which other values of m one has $L = K(\zeta_{2m})$.

References

[AT68] E. Artin, J. Tate, *Class field theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[CT22] A. Cadoret, A. Tamagawa, *Ghosts in families of Abelian varieties with a common isogeny factor*, preprint.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983) 349–366.

[Fit24] F. Fité, *A local-global principle for quadratic twists of abelian varieties*, Math. Ann. **388**, pages 769–794, (2024).

[FP23] F. Fité and A. Perucca, *A local-global principle for polyquadratic twists of abelian surfaces*, to appear in Indiana University Mathematical Journal.

[GGL24] A. Gallese, H. Goodson, D. Lombardo, *Monodromy groups and exceptional Hodge classes*, Arxiv preprint.

[GQ14] X. Guitart, J. Quer, *Modular abelian varieties over number fields*, Canad. J. Math. **66** (2014), 170–196.

[KL20] C.B. Khare and M. Larsen, *Abelian varieties with isogenous reductions*, C. R. Math. Acad. Sci. Paris **358** n. 9-10 (2020), 1085–1089.

[Lan83] S. Lang, *Complex multiplication*, Grundlehren Math. Wiss., **255**, Fundamental Principles of Mathematical Sciences Springer-Verlag, New York, 1983.

[NSW00] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2000.

[Raj98] C.S. Rajan, *On strong multiplicity one for ℓ-adic representations.* Internat. Math. Res. Notices (3) 1998, 161–172.

[Ram00] D. Ramakrishnan, *Recovering modular forms from squares*, appendix to "A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations" by W. Duke and E. Kowalski, Invent. Math. **139** (2000), 1–39.

[Sch77] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arithmetica **32**.3 (1977) 245–274.

[Ser89] Serre, JP. *Local Fields*, Graduate Texts in Mathematics, vol 67. Springer, 1979.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, No. 1, Publ. Math. Soc. Japan, No. 11 Iwanami Shoten Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971.

[Shi98] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton University Press, Princeton, NJ, 1998.

[Was97] L.C. Washington, *Introduction to cyclotomic fields*, Grad. Texts in Math. **83**, Springer-Verlag, New York, 1997.

Institut de Recherche Mathématique Avancée (IRMA), Université de Strasbourg, 7 Rue René Descartes, 67000 Strasbourg

Email address: eambrosi@unistra.fr

URL: http://emiliano.ambrosi.perso.math.cnrs.fr/

Dipartimento di Matematica "Tullio Levi-Civita", Università di Padova, Via Trieste 63, 35132 Padova

Email address: ncoppola@math.unipd.it

URL: https://sites.google.com/view/nirvanacoppola/home

Departament de matemàtiques i informàtica and Centre de recerca matemàtica, Universitat de Barcelona, Gran via de les Corts Catalanes 585, 08007 Barcelona

Email address: ffite@ub.edu

URL: http://www.ub.edu/nt/ffite/