EFFECTIVE SURJECTIVITY OF GALOIS REPRESENTATIONS OF PRODUCTS OF ELLIPTIC CURVES OVER FUNCTION FIELDS

with an appendix with Benjamin Bakker

ALINA CARMEN COJOCARU AND FREDERICK SAIA

Abstract. We prove an effective surjectivity result for Galois representations of products of non-isotrivial, non-isogenous elliptic curves over certain function fields of characteristic 0. This is by way of an isogeny degree bound in this setting, generated from bounds for elliptic curves by Griffon–Pazuki and from the function field analogue of the Frey–Mazur conjecture, by employing techniques originating in work by Serre and Masser–Wüstholz in the number field setting.

1. Introduction

Let K be an arbitrary field with arbitrary characteristic, for which we fix algebraic and separable closures $\overline{K}$ and K^{sep}, and denote by G_K the absolute Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. Let E be an elliptic curve over K and let N be a positive integer. The group G_K acts naturally on the torsion points of E over K^{sep}, acting, in particular, on the subgroup $E[N]$ of points of order dividing N. This action is captured in the mod-N Galois representation

$$\rho_{E,N} : G_K \to \mathrm{GL}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

When K is a number field and E does not have complex multiplication over K^{sep} (shortened as E is non-CM), by a celebrated result of Serre [Ser72, Théorème 2], there exists a constant $c(E/K)$ such that $\rho_{E,\ell}$ is surjective for all primes $\ell > c(E/K)$. Serre also proved an analogous result [Ser72, Théorème 6] for a product of two elliptic curves defined over the number field K, namely that for two non-CM, non-(geometrically)-isogenous elliptic curves E_1 and E_2 over K, there exists a constant $c(E_1/K, E_2/K)$ such that the image of the mod-ℓ Galois representation associated to the product $E_1 \times E_2$ is as large as possible for all primes $\ell > c(E_1/K, E_2/K)$.

When K is the function field of a smooth, projective, and geometrically integral curve over a perfect field of constants k, a theorem of Igusa [Igu59, Theorem 3], whose proof precedes that of Serre's theorem, implies that if E satisfies that $j(E) \notin \overline{k}$, then there exists a constant $c(E/K)$ such that the image of the representation $\rho_{E,\ell}$ is as large as possible, in the sense that $\mathrm{Image}(\rho_{E,\ell}) \cap \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, for all primes $\ell > c(E/K)$. We also refer the reader to [BLV09] for an alternate proof of this result.

Naturally, one asks for effective versions of the above results. Following Serre's work, an effective theorem for the product of an arbitrary number of non-CM, pairwise non-(geometrically)-isogenous elliptic curves elliptic curves $E_1, \ldots, E_n$ over a number field K was proven by Masser–Wüstholz [MW93a, Theorem, Proposition 1] as an application of their work on isogeny degree bounds in [MW93b]. Specifically, Masser–Wüstholz proved that there exists a constant $c(E_1/K, \ldots, E_n/K)$, defined explicitly in terms of the Weil heights of the elliptic curves and the degree of the number field, such that the image of

2020 *Mathematics Subject Classification.* Primary 11G10, Secondary 11G05.

Key words and phrases. Galois representation, elliptic curve, function field, abelian variety, isogeny.

the mod-ℓ Galois representation associated to the product $E_1 \times \ldots \times E_n$ is as large as possible for all primes $\ell > c(E_1/K, \ldots, E_n/K)$. Since their work, the subject of effective surjectivity results over number fields has seen ongoing interest, with many researchers working to improve the bounds of Masser–Wüstholz or to extend these types of results to other classes of abelian varieties (see, e.g., [Coj05, LV14, Lom15, LF16, Lom16b, Lom16a, Zyw22, MW25, MW24]). In the function field setting, an effective surjectivity result for elliptic curves was proven by Cojocaru–Hall in [CH05]. Their theorem, which we recall as Theorem 5.1, shows that, when K is the function field of a smooth, projective, and geometrically integral curve of genus g over a perfect field of constants k, for any elliptic curve E over K with $j(E) \notin \overline{k}$, there exists an explicit constant $c(g)$ such that the image of the representation $\rho_{E,\ell}$ is as large as possible for all primes $\ell \geq c(g)$.

Our main result is an effective surjectivity result for the product of an arbitrary number of elliptic curves over certain function fields, providing the first extension of both Igusa's theorem and Cojocaru–Hall's theorem to abelian varieties of dimension larger than 1. It uses the following notation.

For C a smooth, projective, and geometrically integral curve of genus g over a perfect field k, let $K := k(C)$ denote the function field of C. For $E_1, \ldots, E_n$ elliptic curves over K, consider the product abelian variety of dimension n defined by

$$A := E_1 \times \cdots \times E_n.$$

For any prime $\ell \neq \mathrm{char}(K)$, denote by

$$\rho_{A,\ell} : G_K \to \mathrm{GL}(E_1[\ell] \times \cdots \times E_n[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^n$$

the mod-ℓ Galois representation of A, that is, the product of the mod-ℓ Galois representations of the factors E_i. Since the determinants of the projections of $\rho_{A,\ell}$ to each component must agree, each being equal to the ℓ^{th} cyclotomic character of K, the image of $\rho_{A,\ell}$ is contained in the determinant locus

$$\{(M_1, \ldots, M_n) \mid \det M_1 = \ldots = \det M_n\} \leq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^n.$$

Letting

$$\Psi_\ell(A) := \mathrm{Image}(\rho_{A,\ell}) \cap \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^n,$$

our effective result is as follows (see Theorem 5.3 for a more detailed version):

Theorem 1.1. *Let K be the function field of a smooth, projective, and geometrically integral curve C of genus g over a field k with an embedding $k \hookrightarrow \mathbb{C}$. For $n \geq 2$, let $E_1, \ldots, E_n$ be pairwise non-isogenous elliptic curves over K with $j(E_i) \notin \overline{k}$ for each $1 \leq i \leq n$, and let $A := E_1 \times \cdots \times E_n$. Then there exists a constant $\mathfrak{c}(g)$, depending only on g, such that $\Psi_\ell(A) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^n$ for all primes $\ell > \mathfrak{c}(g)$.*

Similarly to Theorem 5.1, a pleasing aspect of Theorem 1.1 is that the constant $\mathfrak{c}(g)$ depends only on the genus g of the base field and not on the individual elliptic curve factors. In fact, $\mathfrak{c}(g)$ does not even depend on the dimension of A.

It should be possible to make $\mathfrak{c}(g)$ explicit. As we clarify in the statement of Theorem 5.3 (see also Remark 4.7 for related comments), it would suffice to make explicit a result of Bakker–Tsimerman [BT16] which proves a function field analogue of the Frey–Mazur conjecture. Similarly, to obtain from our work a version of Theorem 1.1 over function fields with more general fields of constants, it would suffice to have a version of [BT16, Theorem 2] for such function fields (see Remark 4.6).

Our proof of Theorem 1.1 follows the techniques of Masser–Wüstholz from [MW93a], which, in our setting, require as input an isogeny degree estimate for product abelian surfaces over function fields. This input comes in the form of Corollary 4.5, which we prove by bootstrapping isogeny degree estimates for elliptic curves over function fields,

obtained in recent work of Griffon–Pazuki [GP22, Proposition 6.5, Proposition 6.7]. Our argument, like that of Griffon–Pazuki in the dimension 1 case, involves points on modular curves $X_0(N)$, of specified level N, induced by minimal-degree isogenies, along with genus bounds for $X_0(N)$ in terms of the level N. As hinted above, the argument also uses a variation of an effective version of the Frey–Mazur conjecture in the function field setting [BT16, Corollary 30], proved by Bakker–Tsimerman. Specifically, it relies on a generalization of this result to composite level, handled in Section A and coauthored with Bakker.

Our paper is structured as follows. In Section 2, we briefly review necessary preliminaries related to function fields, heights, and isogenies. In Section 3, we state our generalization of the function-field Frey–Mazur result of Bakker–Tsimerman, which we justify in Section A. We prove isogeny degree bounds in Section 4 and apply one such bound to prove Theorem 1.1 in Section 5.

Acknowledgments. We thank Nathan Jones and Oana Padurariu for feedback on earlier drafts of this work, and we thank Ben Bakker and Ariel Weiss for helpful conversations. We also express our gratitude to the anonymous referees who helped us to identify issues in prior versions of this work, in particular by pointing out errors in a prior version of Proposition 4.4.

2. Background material

2.1. **Function fields and heights.** For the remaining of the paper (with the exception of Section A), unless noted otherwise, K will denote a function field, defined as follows. Let C be a smooth, projective, and geometrically integral curve of genus g over a perfect field k of characteristic $p := \mathrm{char}(k) \geq 0$. We let $K := K(C)$ denote the function field of C and call it a **function field** with **field of constants** k and of **genus** g (noting that g is independent of the choice of model C). While we will later restrict to the case $\mathrm{char}(k) = 0$, we work in general as much as possible to make clear to the reader what would be needed to generalize our main result to nonzero characteristic. For general background on function fields, we refer the reader to [Ros02].

Let L/K be a finite degree extension. For each place w of L, let $|\cdot|_w$ denote the corresponding normalized absolute value on L. Let v denote the unique place of K lying below w and let L_w and K_v, respectively, denote the corresponding completions of L and K. The local degree of w is the quantity

$$n_w := [L_w : K_v].$$

For a point $P = [x_0 : x_1] \in \mathbb{P}^1(L)$, the height of P with respect to L is

$$h_L(P) := \sum_{w \text{ a place of } L} n_w \log \max\{|x_0|_w, |x_1|_w\}.$$

The (absolute logarithmic) **Weil height** of $P \in \mathbb{P}^1(L)$, which is independent of the choice of extension L such that $P \in \mathbb{P}^1(L)$, is defined as

$$h(P) := \frac{h_L(P)}{[L : K]}.$$

For $f \in \overline{K}$, the **Weil height** of f is then defined as

$$h(f) := h([f : 1]).$$

Like results of [MW93a] and [GP22], versions of our effective results on products and isogeny degree bounds will involve the modular heights of elliptic curves. For this purpose, we recall the definition of modular height from [GP22, §1]. The **modular**

height of an elliptic curve E over $\overline{K}$, with j-invariant $j(E)$, is the (absolute logarithmic) Weil height of $j(E)$, that is,

$$\mathrm{h}_{\mathrm{mod}}(E) := h(j(E)).$$

2.2. **Isogenies.** For general background on abelian varieties, we recommend [EvdGM, Mil86, Mum08]. We will most often reference [EvdGM], which from the start works over a general (not necessarily algebraically closed) base field, whenever possible.

Unless otherwise specified, in this paper isogenies will be assumed to be defined over $\overline{K}$ (equivalently, over some finite extension of K).

For abelian varieties X/K and Y/K, of the same dimension $\dim(X) = \dim(Y)$, with respective identity elements 0_X and 0_Y, we let $\mathrm{Hom}_{\overline{K}}(X, Y)$ denote the ring consisting of all isogenies $\left(X \otimes_{\mathrm{Spec}\, K} \mathrm{Spec}\, \overline{K}\right) \to Y \otimes_{\mathrm{Spec}\, K} \mathrm{Spec}\, \overline{K}$ between X and Y over $\overline{K}$, along with the constant map sending every element of X to 0_Y. As a particular case, we let $\mathrm{End}_{\overline{K}}(X)$ denote $\mathrm{Hom}_{\overline{K}}(X, X)$, and for an arbitrary positive integer d, we denote by $[d]_X \in \mathrm{End}_{\overline{K}}(X)$ the multiplication-by-d isogeny. For an isogeny $\varphi \in \mathrm{Hom}_{\overline{K}}(X, Y)$, its degree $\deg(\varphi)$ is the degree $[K(X) : \varphi^*(K(Y))]$ of the corresponding extension of function fields, where $\varphi^* : K(Y) \to K(X)$ denotes the induced pullback map. Equivalently, $\deg(\varphi)$ is the rank of the finite group scheme $\ker(\varphi)$ [EvdGM, p. 73].

The following result is due to Deuring in positive characteristic, and its statement and a proof, which is agnostic to the characteristic, can be found as [GP22, Lemma 2.1].

Lemma 2.1. *Let K be a function field with field of constants k, of arbitrary characteristic, and let E be an elliptic curve over K with $j(E) \notin \overline{k}$. Then* $\mathrm{End}_{\overline{K}}(E) \simeq \mathbb{Z}$.

We call an elliptic curve E/K **isotrivial** if $j(E) \in \overline{k}$, and **non-isotrivial** otherwise. Recalling that an elliptic curve with CM over a number field must have integral j-invariant, the above lemma should be interpreted as an analogue over function fields: if E/K is non-isotrivial (i.e., it has non-constant j-invariant), then it does not have extra endomorphisms.

2.2.1. *Factorizations.* The main thrust of this subsection is to associate to an isogeny an auxiliary isogeny in the other direction; this construction will be relevant to our definition of biseparability to come. Some of the work here is not strictly necessary for the remainder of this paper, but is useful in identifying how one might seek to generalize our isogeny-degree bound in Section 4.

Proposition 2.2. *Let K be a function field of arbitrary characteristic, let X, Y be abelian varieties over K, and let $\varphi \in \mathrm{Hom}_{\overline{K}}(X, Y)$. Let $H \subseteq \ker(\varphi)$ be a subgroup scheme and let $\eta : X \to X/H$ denote the natural quotient map. Then there exists an isogeny $\psi \in \mathrm{Hom}_{\overline{K}}(X/H, Y)$ such that $\varphi = \psi \circ \eta$.*

Proof. The main claim here is the implicit one that X/H is again an abelian variety; this follows from [EvdGM, (4.39) Theorem]. We then get the isogeny ψ from the universal property for quotients. □

The following result will be useful when we need certain factorizations of isogenies to be unique.

Lemma 2.3. [EvdGM, (5.4) Lemma] *Let K be a function field of arbitrary characteristic, let X, Y, Z, W be abelian varieties over K, and let $\alpha \in \mathrm{Hom}_{\overline{K}}(W, X)$, $\beta \in \mathrm{Hom}_{\overline{K}}(Y, Z)$, $\varphi_1, \varphi_2 \in \mathrm{Hom}_{\overline{K}}(X, Y)$ be isogenies such that $\beta \circ \varphi_1 \circ \alpha = \beta \circ \varphi_2 \circ \alpha$. Then $\varphi_1 = \varphi_2$.*

We now introduce for an isogeny φ an associated isogeny $\widetilde{\varphi}$ in the opposite direction.

Proposition 2.4. *Let K be a function field of arbitrary characteristic, let X, Y be abelian varieties over K, and let $\varphi \in \mathrm{Hom}_{\overline{K}}(X, Y)$ be an isogeny of degree d. Then there exists a unique isogeny $\widetilde{\varphi} \in \mathrm{Hom}_{\overline{K}}(Y, X)$ such that*

$$\widetilde{\varphi} \circ \varphi = [d]_X \qquad \text{and} \qquad \varphi \circ \widetilde{\varphi} = [d]_Y.$$

Proof. This is [EvdGM, (5.12) Proposition]. While the uniqueness claim is not explicitly made there, it follows immediately from Lemma 2.3 □

We remark that, when the dimension of X and Y is greater than 1, the isogeny $\widetilde{\varphi}$ is *not* the dual isogeny of φ (note that we have taken care to say nothing about polarizations). In particular, one can see by comparing degrees that the degree of φ is smaller than that of $\widetilde{\varphi}$ in dimension greater than 1, and, as a result, $\widetilde{\widetilde{\varphi}} : X \to Y$ is not equal to φ.

Related to the above remark, we note the following properties, which can be found in [Ros86] for isogenies over $\mathbb{C}$. While Rosen *does* refer to $\widetilde{\varphi}$ as the "dual isogeny," we would label this a misnomer.

Proposition 2.5. *Let K be a function field of arbitrary characteristic, let X, Y, Z be abelian varieties over K of dimension n, and let $\varphi \in \mathrm{Hom}_{\overline{K}}(X, Y)$, $\varphi' \in \mathrm{Hom}_{\overline{K}}(Y, Z)$ be isogenies of degrees d, d', respectively. Then:*

(i) $\deg(\widetilde{\varphi}) = d^{2n-1}$.
(ii) $\widetilde{\widetilde{\varphi}} = [d^{2n-2}]_Y \circ \varphi$.
(iii) $\widetilde{\varphi' \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\varphi'}$.
(iv) For all positive integers m, we have $\widetilde{[m]_X} = [m^{2n-1}]_X$.

Proof. Part (i) is clear from comparing degrees, given that $\widetilde{\varphi} \circ \varphi = [d]_X$ and $\deg([d]_X) = d^{2n}$. For part (ii), note that

$$\begin{aligned} \left([d^{2n-2}]_Y \circ \varphi\right) \circ \widetilde{\varphi} &= [d^{2n-2}]_Y \circ [d]_Y \\ &= [d^{2n-1}]_Y \\ &= \widetilde{\widetilde{\varphi}} \circ \widetilde{\varphi}. \end{aligned}$$

The claim then follows from Lemma 2.3. Part (iii) is seen as follows:

$$\begin{aligned} \left(\widetilde{\varphi} \circ \widetilde{\varphi'}\right) \circ \left(\varphi' \circ \varphi\right) &= \widetilde{\varphi} \circ [d']_Y \circ \varphi \\ &= [dd']_X \\ &= \widetilde{\varphi' \circ \varphi} \circ \left(\varphi' \circ \varphi\right). \end{aligned}$$

Part (iv) is now a routine verification. □

2.2.2. *Separability and biseparability.* We are now ready to introduce our definition of biseparability. For this, let X, Y be abelian varieties over the function field K of arbitrary characteristic and let $\varphi \in \mathrm{Hom}_{\overline{K}}(X, Y)$. We set

$$\deg_{\mathrm{sep}}(\varphi) := [\overline{K}(X) : \varphi^*(\overline{K}(Y))]_{\mathrm{sep}}$$

and

$$\deg_{\mathrm{insep}}(\varphi) := [\overline{K}(X) : \varphi^*(\overline{K}(Y))]_{\mathrm{insep}}$$

to be the separability and inseparability degrees, respectively, of the extension of function fields $\overline{K}(X)/\varphi^*(\overline{K}(Y))$. Equivalently, $\deg_{\mathrm{sep}}(\varphi)$ is equal to the number of closed points of $\ker(\varphi)$ and $\deg_{\mathrm{sep}}(\varphi) \cdot \deg_{\mathrm{insep}}(\varphi) = \deg(\varphi)$. We call φ **separable** if the field extension $\overline{K}(X)/\varphi^*(\overline{K}(Y))$ is separable, i.e., if $\deg_{\mathrm{insep}}(\varphi) = 1$, and **purely inseparable** if this

field extension is purely inseparable, i.e., if $\deg_{\text{sep}}(\varphi) = 1$. We call φ **biseparable** if both φ and $\widetilde{\varphi}$ are separable.

Note that, if $\text{char}(K) = 0$, then all isogenies of abelian varieties over K are separable and hence also biseparable. This does not necessarily hold if $\text{char}(K) > 0$.

Proposition 2.6. [Mum08, Proposition, p.64] *Let K be a function field of positive characteristic $p = \text{char}(K) > 0$, let X be an abelian variety over K of dimension $\dim(X)$, and let d be a positive integer. Then the multiplication-by-d isogeny $[d]_X : X \to X$ is of degree $d^{2\cdot\dim(X)}$, and is separable if and only if d is coprime to p.*

Corollary 2.7. *Let K be a function field of positive characteristic $p = \text{char}(K) > 0$, let X, Y be abelian varieties over K, and let $\varphi \in \text{Hom}_{\overline{K}}(X, Y)$ be an isogeny of degree d. Then φ is biseparable if and only if d is coprime to p.*

Proof. This follows from Proposition 2.6 and the fact that $\widetilde{\varphi} \circ \varphi = [d]_X$. □

Remark 2.8. Our definition of biseparable is a generalization of that from [GP22]. In an effort to be as general as possible and not require polarizations, we believe that working with $\widetilde{\varphi}$ rather than the dual isogeny $\varphi^\vee$ of φ is the right choice in this paper.

Now, let us show that if $p = \text{char}(K) > 0$, then separability does not imply biseparability. As a primary example, for X/K an abelian variety, consider the **Frobenius homomorphism**

$$F_X : X \to X^{(p)},$$

which is purely inseparable, of degree $p^{\dim(X)}$ [EvdGM, Proposition 5.15], and the **Verschiebung homomorphism**

$$V_X : X^{(p)} \to X,$$

which is also of degree $p^{\dim(X)}$. We have that $V_X \circ F_X = [p]_X$, $F_X \circ V_X = [p]_{X^{(p)}}$, and that these homomorphisms are Cartier dual to one-another [EvdGM, Proposition 5.19, Proposition 5.20]. The separability degree of V_X is intimately related to the structure of the p-power torsion of X.

Proposition 2.9. *Let K be a function field of positive characteristic $p = \text{char}(K) > 0$, and let X be an abelian variety over K. Then there exists an integer $r = r(X)$ with $0 \leq r \leq \dim(X)$ such that*

$$X[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})^r$$

for all positive integers m. Explicitly, we have that

$$p^r = \deg_{\text{sep}}(V_X).$$

Moreover, the integer r is invariant under isogeny, that is, if Y is another abelian variety over K such that X is isogenous to Y, then $r(X) = r(Y)$.

Proof. This is [EvdGM, Proposition 5.22]. The fact that $p^r = \deg_{\text{sep}}(V_X)$ is not explicitly stated in their proposition, but is inherent in their proof. □

It is a result of Deuring (see [Mum08, p. 217]) that, in the setting of Proposition 2.9 with X/K an abelian variety of dimension 1, that is, an elliptic curve which we relabel E/K, non-isotriviality is equivalent to $r(E) = 1$. Both properties are therefore equivalent to V_E being separable. In this context, F_E and V_E are dual isogenies, and V_E is a separable isogeny which is not biseparable.

Remaining in the setting of a function field K with $p = \text{char}(K) > 0$, let $E_1, \ldots, E_n$ be non-isotrivial, pairwise non-isogeneous elliptic curves over K and let A be an abelian

variety over K, isogenous to the product $E_1 \times \ldots \times E_n$. Since for any positive integer m, we have

$$(E_1 \times \cdots \times E_n)[p^m] \simeq E_1[p^m] \times \cdots \times E_n[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})^n,$$

we obtain from Proposition 2.9 that $r(A) = n = \dim(A)$. Therefore, once again the Verschiebung V_A is a separable isogeny which is not biseparable. This will be the context of the upcoming results of this paper.

Note that, in the above context, A cannot be defined over a finite field. If there were some finite extension of the field of constants k of K over which we had a model for A, then there would exist some further finite extension over which an isogeny $\varphi : A \to E_1 \times \cdots \times E_n$ is defined. The product $E_1 \times \cdots \times E_n$ must then be defined over said extension, and upon a further finite extension, each E_i would be defined, contradicting our non-isotriviality assumption.

Remark 2.10. The preceding paragraph addresses the case in which A is isogenous to a totally decomposable abelian variety. For simple abelian varieties over a function field K of positive characteristic, a result due to Tate and Grothendieck states that a simple abelian variety over K has a model over a finite field if and only if it is of CM type [Mum08, p. 220]. For elliptic curves, "CM type" is equivalent to isotriviality.

Even though the following lemma will not be explicitly used in what follows, we include it here as it is relevant to the above discussion and we expect that it may be of use in generalizing results of Section 4 to dimension $d > 2$ in positive characteristic.

Lemma 2.11. *Let K be a function field of positive characteristic $p = \mathrm{char}(K) > 0$, let X, Y be abelian varieties over a finite extension L of K, and let $\varphi \in \mathrm{Hom}_{\overline{K}}(X, Y)$ be a biseparable isogeny. Assume that X and Y have no abelian subvarieties of CM type. Then, letting $H := \ker(\varphi)(\overline{K})$, we have that $L(H)/L$ is a separable field extension.*

Proof. This proof follows similarly to that in [GP22, Lemma 4.6]: setting $d = \deg(\varphi)$, we know that $H \subseteq X[d]$, and because d is coprime to p, it follows from [ST68, §1] that $L(X[d])/L$ is separable. Hence, $L(H)/L$ is separable. □

3. Congruences of elliptic curves over function fields

In this section, we recall a bound due to Bakker–Tsimerman related to congruences of elliptic curves over function fields, which we will use in the following section. First, we recall the notion of an N-congruence of elliptic curves.

Let N be a positive integer and let E_1, E_2 be elliptic curves over an arbitrary field F of characteristic not dividing N. An **N-congruence** between E_1 and E_2 is an isomorphism of G_F-modules between $E_1[N]$ and $E_2[N]$.

The Frey–Mazur conjecture states that there exists a constant N_0 such that there exists no N-congruence between elliptic curves over $\mathbb{Q}$ for all integers $N > N_0$. We refer the reader to [Fis14, §1], [FK22, §1.2], and [Fre24, §1] as useful sources for background on this conjecture and related work. For the natural analogue of the Frey–Mazur conjecture in the function field setting, we have the following effective result of Bakker–Tsimerman.

Theorem 3.1. [BT16, Theorem 2] *Let K be the function field of a smooth, projective, and irreducible[1] curve of genus g over $\mathbb{C}$. Let E_1, E_2 be non-isotrivial, non-isogenous elliptic curves over K. There exists a constant $\mathcal{N}(g)$, depending only on g, such that if there exists an N-congruence between E_1 and E_2, then $N \leq \mathcal{N}(g)$.*

[1]Given that we are working over an algebraically closed field, a curve being irreducible is equivalent to being geometrically integral.

Remark 3.2. The exact statement of Theorem 3.1 in [BT16] only gives a bound which excludes N-congruences of elliptic curves over K for sufficiently large primes N, though their methods can be adapted to give the result for general positive integers N. While this is not particularly surprising, it is perhaps best to give some details on this extension, which we do in Section A. The main result in [BT16] also is phrased in terms of the gonality of K, rather than the genus, but again their methods are suitable to give a bound as in Theorem 3.1 (this is weaker, and immediately follows from their statement [BT16, Corollary 30]). We are satisfied with this dependency, as other results we will use have a similar dependence on the genus.

Remark 3.3. Because the degrees of cyclic isogenies of non-isotrivial elliptic curves over a function field K are uniformly bounded in terms of the genus of K (see Proposition 4.2), the "non-isogenous" hypothesis in Theorem 3.1 is not necessary (though the required constant $\mathcal{N}(g)$ may increase upon dropping this hypothesis). We prefer the statement above for this paper, as we will always work with non-isogenous curves.

4. An isogeny degree bound

As in Section 2, let C be a smooth, projective, and geometrically integral curve of genus g over a perfect field k of characteristic $p := \mathrm{char}(k) \geq 0$, and consider the function field $K = K(C)$.

The following statement, providing an upper bound on the order of a G_K-stable subgroup of an elliptic curve over K in terms of just the genus of K, is [GP22, Proposition 6.5]. It is deduced from a clever observation that, in the function field setting, a K-rational point on the modular curve $X_0(d)$ induces a morphism $C \to X_0(d)$ from our smooth model C of K to $X_0(d)$ over the constant field k.

Lemma 4.1. *Let K be a function field of arbitrary characteristic and genus g, let E be a non-isotrivial elliptic curve over K, and let $H \subseteq E$ be a cyclic, G_K-stable subgroup of order d. If d is coprime to* $\mathrm{char}(K)$*, then*

$$d \leq 49 \cdot \max\{1, g\}.$$

In their work, Griffon–Pazuki use Lemma 4.1 to obtain the following degree bounds for biseparable isogenies of elliptic curves over function fields.

Proposition 4.2. [GP22, Proposition 6.7] *Let K be a function field of arbitrary characteristic and genus g, and let E_1, E_2 be two non-isotrivial elliptic curves over K. Assume that there exists a biseparable isogeny $\varphi \in \mathrm{Hom}_{\overline{K}}(E_1, E_2)$ defined over K. Then there exists a biseparable isogeny $\varphi_0 \in \mathrm{Hom}_{\overline{K}}(E_1, E_2)$ defined over K with*

$$\deg(\varphi_0) \leq 49 \cdot \max\{1, g\}.$$

Proposition 4.3. *Let K be a function field of arbitrary characteristic, let L/K be a finite extension, and let E_1, E_2 be two non-isotrivial elliptic curves over L. Assume that there exists a biseparable isogeny $\varphi \in \mathrm{Hom}_{\overline{K}}(E_1, E_2)$ defined over L. Then there exists a biseparable isogeny $\varphi_0 \in \mathrm{Hom}_{\overline{K}}(E_1, E_2)$ defined over L with*

$$\deg(\varphi_0) \leq [L : K] \cdot \min\{\mathrm{h}_{\mathrm{mod}}(E_1), \mathrm{h}_{\mathrm{mod}}(E_2)\}.$$

Proof. This follows from the same argument given for [GP22, Proposition 6.7], but using the cruder degree bound of [GP22, Proposition 6.6] in place of [GP22, Proposition 6.5]. □

In the following proposition and its corollary, we leverage Proposition 4.2 and Theorem 3.1 to obtain analogous results for a product of two elliptic curves.

Proposition 4.4. *Let K be a function field of arbitrary characteristic and genus g, let E_1, E_2 be non-isotrivial, non-isogenous elliptic curves over K, with identity elements denoted $0_1, 0_2$, respectively, and let X be an abelian surface over K. Assume that there exists a biseparable isogeny $\varphi \in \mathrm{Hom}_{\overline{K}}(E_1 \times E_2, X)$ defined over K and let φ_0 be such an isogeny of minimal degree. Setting*

$$E_1' := \varphi_0\left(E_1 \times \{0_2\}\right), \quad E_2' := \varphi_0\left(\{0_1\} \times E_2\right),$$

we have

$$\deg(\varphi_0) \leq 49^2 \cdot |(E_1' \cap E_2')(\overline{K})| \cdot \max\{1, g^2\}.$$

Proof. The start of our proof will be similar to that of [GP22, Proposition 6.7], with the added task of relating our isogeny degree bound to induced points on modular curves. We begin by clarifying our setup.

Set

$$d_0 := \min\{d \in \mathbb{Z}^+ \mid \exists \text{ a biseparable isogeny } E_1 \times E_2 \to X \text{ of degree } d \text{ over } K\}.$$

This integer is well-defined thanks to our hypothesis that there exists a biseparable isogeny over K between the abelian surfaces $E_1 \times E_2$ and X. In fact, d_0 is the degree of the biseparable isogeny of minimal degree, $\varphi_0 : E_1 \times E_2 \to X$. By Corollary 2.7, we must have $p \nmid d_0$ if $p = \mathrm{char}(K) > 0$.

Each of the elliptic curves E_1', E_2' is an abelian subvariety of X. Considering the isogenies $\varphi_1 : E_1 \longrightarrow E_1'$, $P_1 \longmapsto \varphi_0(P_1, 0_2)$, and $\varphi_2 : E_2 \longrightarrow E_2'$, $P_2 \longmapsto \varphi_0(0_1, P_2)$, we see that $\ker(\varphi_1)(\overline{K}) \times \{0_2\} \leq \ker(\varphi_0)(\overline{K})$ and $\{0_1\} \times \ker(\varphi_2)(\overline{K}) \leq \ker(\varphi_0)(\overline{K})$. Moreover, if $(P_1, P_2) \in \ker(\varphi_0)(\overline{K})$, then, with 0_X denoting the identity of X, we find that $\varphi_1(P_1) + \varphi_2(P_2) = \varphi_0(P_1, P_2) = 0_X$, or equivalently $\varphi_1(P_1) = \varphi_2(-P_2)$. Consequently, we have $\varphi_1(P_1) \in (E_1' \cap E_2')(\overline{K})$.

For a given point $R \in E_1' \cap E_2'$ and for each $1 \leq i \leq 2$, there are $d_i := \deg(\phi_i)$ points $P_i \in E_i$ with $\varphi_i(P_i) = R$. Moreover, each pair of points $(P_1, P_2) \in E_1(\overline{K}) \times E_2(\overline{K})$ satisfying $\varphi_1(P_1) = \varphi_2(P_2) = R$ also satisfies $(P_1, P_2) \in \ker(\varphi_0)(\overline{K})$.

The fact that E_1 and E_2 are non-isogenous implies that $|(E_1' \cap E_2')(\overline{K})|$ is finite (as E_1 and E_2 are irreducible curves, if they intersect at infinitely many points then they must in fact be identical). Then, in light of the above observations, we obtain that

$$d_0 = |\ker(\varphi_0)(\overline{K})| = d_1 d_2 \cdot |(E_1' \cap E_2')(\overline{K})|. \tag{4.1}$$

Recalling that if $p = \mathrm{char}(K) > 0$, we have $p \nmid d_0$, we also have $p \nmid d_i$ for each $1 \leq i \leq 2$.

We claim that both φ_1 and φ_2 are cyclic isogenies of elliptic curves. Suppose, for example, that φ_1 is not cyclic, so there exists some integer $m > 1$ such that $m \mid d_1$ and φ_1 factors through the endomorphism $[m]_{E_1} : E_1 \to E_1$. It follows that φ_0 factors through the endomorphism

$$\eta := [m]_{E_1} \times \mathrm{Id}_{E_2} \in \mathrm{End}_{\overline{\mathbb{Q}}}(E_1 \times E_2) \simeq \mathbb{Z}^2.$$

Then, by Proposition 2.2, there exists an isogeny $\psi : E_1 \times E_2 \to X$ with $\varphi_0 = \psi \circ \eta$. By comparing degrees, we find that ψ is both biseparable and of degree strictly less than d_0, contradicting the minimality of the degree of φ_0.

Now, by the same arguments as in the proof of [GP22, Proposition 6.7] and the fact that $d_1, d_2 \mid d_0$, both φ_1 and φ_2 are cyclic and biseparable with kernel stable under the action of G_K. Thus, for each $1 \leq i \leq 2$, φ_i induces a K-rational point on $X_0(d_i)$. Lemma 4.1 then provides the inequalities

$$d_i \leq 49 \cdot \max\{1, g\},$$

which, used in (4.1), complete the proof. □

Corollary 4.5. *Let K be a function field of of a smooth, projective, irreducible curve C of genus g over a field k with an embedding $k \hookrightarrow \mathbb{C}$, let E_1, E_2 be non-isotrivial, non-isogenous elliptic curves over K, and let X be an abelian surface over K. Assume that there exists a biseparable isogeny $\varphi \in \mathrm{Hom}_{\overline{K}}(E_1 \times E_2, X)$ defined over K. Then there exists an isogeny $\varphi_0 \in \mathrm{Hom}_{\overline{K}}(E_1 \times E_2, X)$ defined over K with*

$$\deg(\varphi_0) \leq 49^3 \cdot \mathcal{N}(g)^2 \cdot \max\{1, g^3\},$$

where $\mathcal{N}(g)$ is the constant introduced in Theorem 3.1.

Proof. From Proposition 4.4, it remains to bound $|(E_1' \cap E_2')(\overline{K})|$, with E_1' and E_2' as defined therein.

First, note that the intersection $(E_1' \cap E_2')(\overline{K})$ is stable under the action of G_K: if $\sigma \in G_K$ and R is an element of this intersection, then we can take points $P_1 \in E_1(\overline{K})$ and $P_2 \in E_2(\overline{K})$ with $\varphi_1(P_1) = \varphi_2(P_2) = R$, obtaining that

$$R^\sigma = \varphi_1(P_1^\sigma) = \varphi_2(P_2^\sigma).$$

Since this intersection is finite, it is contained in the torsion subgroup of the base change of each E_i to some finite extension of K. Thus, there exist positive integers $M \mid N$ such that

$$(E_1' \cap E_2')(\overline{K}) \simeq \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

as groups. This isomorphism yields two useful pieces of information:

- there exists an M-congruence between E_1' and E_2' over K, and
- each E_i' has a cyclic N/M-isogeny defined over K.[2]

From the first item, we know by Theorem 3.1 that $M \leq \mathcal{N}(g)$ (this is where it is needed that k embeds into $\mathbb{C}$). The second item implies by Proposition 4.2 that

$$N/M \leq 49 \cdot \max\{1, g\}.$$

Putting this together, we obtain that

$$|(E_1' \cap E_2')(\overline{K})| = M^2 \cdot (N/M) \leq 49 \cdot \mathcal{N}(g)^2 \cdot \max\{1, g\},$$

and so from Proposition 4.4 we deduce the stated result. □

Remark 4.6. We separate Proposition 4.4 and Corollary 4.5 into two statements in part to note that the assumption that k embeds into $\mathbb{C}$ in the latter is only required for the application of Theorem 3.1. If one had a version of the bound in Theorem 3.1 over a given field of constants k of arbitrary characteristic, then one could generalize Corollary 4.5 accordingly (upon restriction to biseparable isogenies). We hope that this separation also makes clear how one could get a smaller non-uniform bound for certain fixed E_1, E_2, and X out of Proposition 4.4 if one had a biseparable isogeny $E_1 \times E_2 \to X$ with small intersection $(E_1' \cap E_2')(\overline{K})$.

Remark 4.7. We write the bound in Corollary 4.5 without absorbing all factors into a single constant to make it clear that the only non-explicit component of this bound is the constant $\mathcal{N}(g)$ coming from Theorem 3.1. This is true for all of our results in this paper depending on $\mathcal{N}(g)$: all bounds can be made explicit upon making the bound $\mathcal{N}(g)$ explicit. One of the authors of [BT16] mentioned to us that it should be possible to make their bound explicit following their methods. We do not pursue this task in this paper.

[2] This is because the group $(E_1' \cap E_2')(\overline{K})$, being isomorphic to $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, has a unique cyclic order N/M subgroup which is contained in all of its cyclic order N subgroups. Namely, this is the intersection of all of the cyclic order N subgroups. This cyclic order N/M subgroup must then also be G_K-stable.

We also provide a version of Proposition 4.4 in terms of modular heights, similar to Proposition 4.3.

Proposition 4.8. *Let K be a function field of arbitrary characteristic, let L be a finite extension of K, let E_1, E_2 be non-isotrivial, non-isogenous elliptic curves over L, and let X be an abelian surface over L. Assume that there exists a biseparable isogeny $\varphi \in \mathrm{Hom}_{\overline{K}}(E_1 \times E_2, X)$ defined over L. Then there exists a biseparable isogeny $\varphi_0 \in \mathrm{Hom}_{\overline{K}}(E_1 \times E_2, X)$ defined over L with*

$$\deg(\varphi_0) \leq [L : K]^2 \cdot \mathrm{h}_{\mathrm{mod}}(E_1) \cdot \mathrm{h}_{\mathrm{mod}}(E_2) \cdot |(E_1' \cap E_2')(\overline{K})|,$$

where $E_1' := \varphi_0(E_1 \times \{0_2\})$, $E_2' := \varphi_0(\{0_1\} \times E_2)$, with $0_1, 0_2$ denoting the identity elements of E_1, E_2, respectively.

Proof. One need only apply [GP22, Proposition 6.6] in place of Lemma 4.1 in the proof of Proposition 4.4, as was done to obtain Proposition 4.3 compared to Proposition 4.2 in the elliptic curve case. □

While Proposition 4.2 and Corollary 4.5 have the pleasing feature of uniformity in the elliptic curves E_1, E_2 and abelian surface X, depending only on the genus of K, their non-uniform counterparts Proposition 4.3 and Proposition 4.8 are also valuable. For instance, Griffon–Pazuki use Proposition 4.3 to prove a bound on sizes of isogeny classes over fixed degrees [GP22, Proposition 6.12]; for their purpose, Proposition 4.2 is too crude, as genera may be unbounded over a family of extensions of K of a fixed degree.

5. Effective surjectivity for products

In this section, we apply the results of Section 4 to obtain an effective open image-type result for Galois representations of products of elliptic curves over a function field. An effective result in the case of a single elliptic curve was obtained by Cojocaru–Hall [CH05, Theorem 1.1], and we will make use of their theorem here. To state it, we recall the following setup.

Let C be a smooth, projective, and geometrically integral curve of genus g over a perfect field k of characteristic $p := \mathrm{char}(k) \geq 0$, and consider the function field $K = K(C)$. For E an elliptic curve over K and ℓ a rational prime not equal to $\mathrm{char}(K)$, let

$$\rho_{E,\ell} : G_K \to \mathrm{GL}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

denote the mod-ℓ Galois representation of E, obtained via the action of G_K on the ℓ-torsion points of E. (The isomorphism with $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ here is non-canonical, depending on a choice of basis for $E[\ell]$.) Letting

$$\chi_\ell : G_K \to (\mathbb{Z}/\ell\mathbb{Z})^\times$$

denote the ℓ^{th} cyclotomic character of K, we have that $\det \circ \rho_{E,\ell} = \chi_\ell$. Hence, the image $\mathrm{Image}(\rho_{E,\ell})$ must be a subgroup of the group $\Gamma_\ell \leq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ determined by the short exact sequence

$$0 \to \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to \Gamma_\ell \to \chi_\ell(G_K) \to 0.$$

That is, Γ_ℓ is the inverse image in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of the determinant map. Following [CH05, §1], we call

$$\Psi_\ell(E) := \mathrm{Image}(\rho_{E,\ell}) \cap \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq \Gamma_\ell \cap \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

the **geometric Galois group** of $K(E[\ell])/K$. The fixed field of $\Psi_\ell(E)$ corresponds to the constant extension $(K(E[\ell]) \cap \overline{k})K/K$ obtained by adjoining a primitive ℓ^{th} root of unity, and is invariant under a change in K by a constant extension in this setup (hence the adjective "geometric" here). In other words, we have $\mathrm{Image}(\rho_{E,\ell}) = \Psi_\ell(E)$ upon a

base change of C from k to a cyclotomic extension of k, and so we restrict our attention to $\Psi_\ell(E)$ for a geometric result. Specifically, the effective result of Cojocaru–Hall states that $\Psi_\ell(E)$ is all of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for sufficiently large primes ℓ, where "sufficiently large" depends only on the genus of K.

Theorem 5.1. [CH05, Theorem 1.1] *Let K be a function field of arbitrary characteristic and genus g. Define*

$$c(g) := 2 + \max\left\{q \text{ prime} \;\middle|\; \frac{q - (6 + 3e_2(q) + 4e_3(q))}{12} \leq g\right\},$$

where, for an arbitrary prime q,

$$e_2(q) := \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4, \\ -1 & \text{otherwise,} \end{cases} \quad \text{and} \quad e_3(q) := \begin{cases} 1 & \text{if } q \equiv 1 \pmod 3, \\ -1 & \text{otherwise.} \end{cases}$$

Let E be a non-isotrivial elliptic curve over K. Then $\Psi_\ell(E) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell \geq c(g)$ with $\ell \neq \mathrm{char}(K)$.

To get an effective surjectivity bound for products of such elliptic curves over K, we follow the techniques of Masser–Wüstholz [MW93a]. In the referenced work, the authors use an upgraded version [MW93a, Lemma 2.2] of an isogeny degree bound from their prior work [MW93b] both to prove a result for one single elliptic curve over a number field [MW93a, Theorem], analogous to Theorem 5.1, and to bootstrap this version to products of an arbitrary number of elliptic curves over a number field [MW93a, Proposition 1]. We will proceed similarly, utilizing instead our isogeny degree bound in the function field setting Corollary 4.5.

The following algebraic result of Masser–Wüstholz, which is a slight generalization of a result of Serre [Ser72, Lemme 8], will be useful in the course of our proof.

Lemma 5.2. [MW93a, Lemma 5.1] *Let $\ell \geq 5$ be a prime, let e be a divisor of $\ell - 1$, let V_1, V_2 be vector spaces of dimension 2 over $\mathbb{F}_\ell$, and let B_1, B_2 be the subgroups of $\mathrm{GL}(V_1)$, $\mathrm{GL}(V_2)$, respectively, consisting of all elements whose determinants are e^{th} powers. Let D be the subgroup of $B_1 \times B_2$ consisting of all pairs (b_1, b_2) with $\det b_1 = \det b_2$, and suppose H is a subgroup of D in $B_1 \times B_2$ whose projections to each factor are surjective. If $H \neq D$, then there is an isomorphism $f : V_1 \longrightarrow V_2$ and a character χ of H with $\chi^2 = 1$ such that*

$$b_2 = \chi(h) f b_1 f^{-1}$$

for all $h = (b_1, b_2) \in H$.

We are ready to state and prove our main theorem.

Theorem 5.3. *Let $K = K(C)$ be the function field of a smooth, projective, and geometrically integral curve C of genus g over a field k with an embedding $k \hookrightarrow \mathbb{C}$. Define*

$$\mathfrak{c}(g) = 40353607 \cdot \mathcal{N}(g)^3 \cdot \max\{1, g^{9/2}\},$$

where $\mathcal{N}(g)$ is the constant introduced in Theorem 3.1. Let $n \geq 2$, let $E_1, \ldots, E_n$ be non-isotrivial, pairwise non-isogenous elliptic curves over K, and let $A := E_1 \times \cdots \times E_n$. For an arbitrary prime ℓ, denote by

$$\begin{aligned} \rho_{A,\ell} : G_K &\longrightarrow \mathrm{GL}(E_1[\ell]) \times \cdots \times \mathrm{GL}(E_n[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^n \\ \sigma &\longmapsto (\rho_{E_1,\ell}(\sigma), \ldots, \rho_{E_n,\ell}(\sigma)), \end{aligned}$$

the mod-ℓ Galois representation of A, and set $\Psi_\ell(A) := \mathrm{Image}(\rho_{A,\ell}) \cap \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^n$. Then $\Psi_\ell(A) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^n$ for all primes $\ell > \mathfrak{c}(g)$.

Proof. We follow the proof structure of [MW93a, Proposition 1]. We circumvent the dependence on the number field setting in the proof of this referenced result by utilizing our function field ingredients Theorem 5.1 and Corollary 4.5.

First, we handle the case $n = 2$ of a product of two elliptic curves. Let E_1 and E_2 be two non-isotrivial, non-isogenous elliptic curves over K, and let ℓ be a prime satisfying $\ell \geq c(g)$. Note that it follows that $\ell \geq c(0) = 17$. Take $H := \mathrm{Image}(\rho_{E_1 \times E_2, \ell})$, $V_1 := E_1[\ell]$, and $V_2 = E_2[\ell]$. We deduce from Theorem 5.1 that H projects surjectively onto $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ in each factor of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^2$.

We may then apply Lemma 5.2 with the above H, V_1 and V_2 (the correct divisor $e \mid (\ell - 1)$ is determined by this setup as described in [MW93a, p. 251], while B_1, B_2, and D are as described in the statement of the referenced lemma). If $H = D$, then we are done. Otherwise, we have an isomorphism $f : V_1 \to V_2$ and a character χ_0 on G_K, induced from the character χ on H given by the lemma, such that, for every $\sigma \in G_K$,

$$\rho_{E_2,\ell}(\sigma) = \chi_0(\sigma) f \rho_{E_1,\ell}(\sigma) f^{-1}.$$

This means that f induces a G_K-module isomorphism

$$f_{\chi_0} : E_1[\ell] \longrightarrow E_{2,\chi_0}[\ell],$$

where E_{2,χ_0} is the quadratic twist of E_2 by χ_0; so, for every $\sigma \in G_K$,

$$\rho_{E_{2,\chi_0},\ell}(\sigma) = f_{\chi_0} \rho_{E_1,\ell}(\sigma) f_{\chi_0}^{-1}.$$

We note that

$$\Gamma := \{(x, f_{\chi_0} x) \in E_1 \times E_{2,\chi_0} \mid x \in E_1[\ell]\}$$

is a subgroup of $E_1 \times E_{2,\chi_0}$ stable under the action of G_K. Indeed, if $\sigma \in G_K$ and $y := \rho_{E_1,\ell}(\sigma) x$, then

$$\sigma(x, f_{\chi_0} x) = (\rho_{E_1,\ell}(\sigma) x, \rho_{E_{2,\chi_0},\ell}(\sigma) f_{\chi_0} x) = (y, f_{\chi_0} y) \in \Gamma.$$

Therefore, the abelian surfaces $E_1 \times E_{2,\chi_0}$ and $(E_1 \times E_{2,\chi_0})/\Gamma$ are both defined over K and are isogenous via the natural quotient map $\pi : E_1 \times E_{2,\chi_0} \to (E_1 \times E_{2,\chi_0})/\Gamma$.

By our assumptions on E_1, E_2 and k, Corollary 4.5 provides the existence of an isogeny

$$\psi_0 : E_1 \times E_{2,\chi_0} \to (E_1 \times E_{2,\chi_0})/\Gamma$$

with

$$\deg(\psi_0) \leq 49^3 \cdot \mathcal{N}(g)^2 \cdot \max\{1, g^3\}.$$

We then have an endomorphism

$$\epsilon := \widetilde{\psi_0} \circ \pi \in \mathrm{End}_{\overline{K}}(E_1 \times E_{2,\chi_0}) \simeq \mathbb{Z}^2$$

of degree $\ell^2 \cdot \deg(\psi_0)^3$, which we can represent by a matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ for some $a, b \in \mathbb{Z}$. As π annihilates Γ, so too does ϵ, and so for all $x \in E_1[\ell]$ we have

$$ax = b f_{\chi_0} x = 0.$$

This means that the multiplication-by-a map on E_1 and the multiplication-by-b map on E_{2,χ_0} both annihilate the ℓ-torsion (as f_{χ_0} is an isomorphism), and so $\ell \mid a$ and $\ell \mid b$. Moreover, $\ell^4 \mid a^2 b^2 = \deg(\epsilon)$, so $\ell^2 \mid \deg(\psi_0)^3$. We can then rule out this case by assuming that

$$\ell > 40353607 \cdot \mathcal{N}(g)^3 \cdot \max\{1, g^{9/2}\},$$

which we now do. Thus, for all primes

$$\begin{aligned}\ell &> 40353607 \cdot \mathcal{N}(g)^3 \cdot \max\{1, g^{9/2}\} \\ &= \max\left\{c(g), 40353607 \cdot \mathcal{N}(g)^3 \cdot \max\{1, g^{9/2}\}\right\},\end{aligned}$$

we have the desired equality $\Psi_\ell(E_1 \times E_2) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^2$.

We obtain the general case from the $n = 2$ case, as follows. Let $E_1, E_2, \ldots, E_n$ be non-isotrivial, pairwise non-isogenous elliptic curves over K, and let ℓ be a prime satisfying $\ell > \mathfrak{c}(g)$. By the previous case of a product of two elliptic curves, the image of the map from $\Psi_\ell(E_1 \times E_2 \times \ldots \times E_n)$ to $\mathrm{SL}(\mathbb{Z}/\ell\mathbb{Z})^2$ via the projection of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^n$ onto any two distinct factors is surjective. As in the proof of [MW93a, Proposition 1], we now use the result of Ribet [Rib76, Lemma 5.2.2] which implies that $\Psi_\ell(E_1 \times E_2 \times \ldots \times E_n) = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})^n$ (noting that $\ell > c(0) = 17 > 5$). This completes the proof of our main theorem. □

Remark 5.4. In our setup for Theorem 5.3 (see also Theorem 1.1 stated in the introduction), we assume that $\dim(A) = n \geq 2$. The fact that $\mathfrak{c}(g) \geq c(g)$ for all g allows the flexibility of assuming $n \geq 1$. Of course, in the $n = 1$ case, $\mathfrak{c}(g)$ can be a cruder bound, in which case one should defer to the bound $c(g)$ from Theorem 5.1.

Remark 5.5. We thank Ariel Weiss for pointing out to us that the character χ_0 in the proof of Theorem 5.3 yields an isogeny over K with source the abelian surface $E_1 \times E_{2,\chi_0}$. While Serre notes that the isomorphism f yields an isomorphism between the ℓ-torsion subgroups of E_1 and the twist E_{2,χ_0} [Ser72, p. 328], Masser–Wüstholz trivialize χ_0 to get an isogeny over the extension K^{χ_0}/K, of degree at most 2, instead of using the associated isogeny of abelian surfaces over K as in our proof. Using their isogeny estimates, this line of argument only costs Masser–Wüstholz a factor of 2 in their final bound compared to the argument that we use. For us, the argument over K importantly allows us to forego other possible arguments limiting the ramification of the characters that show up, which would be needed for the uniform version Theorem 5.3; the character χ_0 depends on ℓ, and it is not immediately clear that the extensions K^{χ_0}/K obtained as one ranges over ℓ have uniformly bounded genus.

Appendix A. Function Field Frey–Mazur at Composite Level (with Benjamin Bakker)

A.1. **Introduction and strategy.** This appendix is devoted to the extension of Bakker–Tsimerman's Frey–Mazur result over function fields over $\mathbb{C}$ [BT16, Corollary 30] to composite level, as we stated in Section 3 and used in Section 4. While an extension of their main results in terms of the gonality of the base field [BT16, Theorem 2, Theorem 3] should also be achievable via the methods used in their paper, we only require for our purposes a result in terms of the genus of the base field as in Theorem 3.1. We restrict to this result, which we recall below, for brevity of this appendix.

Theorem A.1 (cf. [BT16, Theorem 2])**.** *Let K be the function field of a smooth, projective, and irreducible curve C of genus g over $\mathbb{C}$. Let E_1 and E_2 be non-isotrivial, non-isogenous elliptic curves over K. There exists a constant $\mathcal{N}(g)$, depending only on g, such that if there exists an N-congruence between E_1 and E_2, then $N \leq \mathcal{N}(g)$.*

We briefly recall here the strategy of [BT16], and refer the reader to this referenced work for further background and details. The authors consider over $\mathbb{C}$ the surface $Z(N)$ parameterizing N-congruences of elliptic curves, which is realized as the quotient of

$X(N) \times X(N)$ by the diagonal action of $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. Here, $X(N)$ is the modular curve parameterizing elliptic curves E with a choice of projective isomorphism $E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$. An N-congruence of elliptic curves $E_1[N] \simeq E_2[N]$ over a function field K over $\mathbb{C}$, with model C, implies the existence of a map $C \to Z(N)$ over $\mathbb{C}$, and Theorem A.1 is then equivalent to the statement that any such curve C of significantly large genus (or, in their case, gonality) must live on a Hecke divisor H_M in $Z(N)$, which parameterizes congruences between M-isogenous elliptic curves.

Working in terms of the gonality γ of the function field K, the authors take a gonal map $C \to \mathbb{P}^1$, which provides a map $\mathbb{P}^1 \to \mathrm{Sym}^\gamma(Z(N))$ to the symmetric product of $Z(N)$, and then lift this to a map

$$C \to (X(N) \times X(N))^\gamma .$$

They estimate the genus of C in two ways in order to reach a contradiction for $N = p$ a significantly large prime, with the main work going into bounding the ramification of $C \to \mathbb{P}^1$ by showing that the ramification points of the map

$$(X(p) \times X(p))^\gamma \to \mathrm{Sym}^\gamma(Z(p))$$

have small incidence with C. This is done via the multiplicity estimates of [BT16, Section 6], which in turn are fed by results that special points on curves in $X(p) \times X(p)$ tend to repel from [BT16, Section 4] and from general volume estimates for special subvarieties in hyperbolic manifolds proven in [BT16, Section 5].

A.2. **The requisite machinery.** In this section, which is the technical heart of this appendix, we generalize the necessary results from [BT16] to prime-power levels. Once obtained, these will lead to a quick proof of Theorem A.1 along the same lines of the proof of the main theorem in the referenced work. In all that follows, we adopt the notation and conventions from [BT16, §1.3], in particular regarding asymptotics and metrics, departing, as needed, from the notation of the previous sections of our paper. We emphasize that the letters p and k are now used for an arbitrary prime and an arbitrary positive integer, respectively, while g denotes either a group element or a non-negative integer.

We begin by borrowing terminology from [BT16, §2.4] for ramification points of the natural map $X(N) \times X(N) \to Z(N)$.

Definition A.2. Let $x, y \in X(N)$ be CM points induced by pairs (E_x, φ_x), (E_y, φ_y), and suppose that x and y have a common non-trivial stabilizer element $g \in \mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. Take lifts $g_x, g_y \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of g and automorphisms h_x, h_y of E_x, E_y, respectively, having the same characteristic polynomial such that

$$h_x \circ \varphi_x = \varphi_x \circ g_x^{-1},$$

and similarly with x replaced by y. We call the point $(x, y) \in X(N) \times X(N)$ a **Heegner CM point** if the eigenvalues of the action of h_x, h_y on the tangent spaces T_0E_x, T_0E_y are the same, and an **anti-Heegner CM point** otherwise. When the level N is clear from context, we denote the sets of Heegner CM points and anti–Hegner CM points on $X(N) \times X(N)$ by $\mathrm{CM}^+, \mathrm{CM}^-$, respectively, and we set

$$\mathrm{CM} := \mathrm{CM}^+ \cup \mathrm{CM}^-.$$

Definition A.3. We call a point $(x, y) \in X(N) \times X(N)$ a **singular bicusp** if x, y are cusps on $X(N)$ sharing a non-trivial stabilizer in $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. When the level N is clear from context, we denote the set of singular bicusps on $X(N) \times X(N)$ by SBC.

A.2.1. *Injectivity radii and heights.* Recall that the **injectivity radius** $\rho_C(x)$ of a compact hyperbolic curve C at a point $x \in C$ is half the minimum length of a geodesic loop based at x, and the **injectivity radius** ρ_C of C is the minimum

$$\rho_C := \min_{x \in C} \rho_C(x).$$

First and foremost, we have the following:

Lemma A.4. *Equip $X(N)$ with its hyperbolic metric of constant sectional curvature -1. Then*

$$\rho_{X(N)} = 2 \log N + O(1)$$

Proof. See [BT16, Corollary 8]. The arguments therein do not require that N is prime. □

Note also that the height estimates from [BT16, §3.3] similarly generalize to $X(N)$; we leave this to the reader.

We view $X(N)$ as a Galois étale cover of $X(1)_N := \Gamma(2,3,N)\backslash\mathbb{H}$ with Galois group $G(N) \simeq \mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$, where $\Gamma(2,3,N)$ is the triangle group with vertices $i, e^{i\theta_N}, iy_N$. The natural map $Y(1) \to X(1)_N$ gives a map on fundamental groups $\mathrm{PSL}_2(\mathbb{Z}) \to \Gamma(2,3,N)$, which induces an isomorphism $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z}) \to G(N)$ that we suppress from the notation. Let $\iota, \varpi, \mathfrak{y} \in X(N)$ be the images of $i, e^{i\theta_N}, iy_N \in \mathbb{H}$ and let $\bar{H} \subset G(N)$ be the stabilizer of $\mathfrak{y}$.

A.2.2. *Repulsion of CM points and multiplicities.*

Lemma A.5 (cf. [BT16, Proposition 14])**.** *For any sufficiently small $\delta > 0$, any prime p, and any sufficiently large positive integer k, we have the following. Let $\xi, \xi' \in X(p^k) \times X(p^k)$ be distinct Heegner CM points points which have the same projections in $X(1) \times X(1)$. If $d(\xi, \xi') < \delta \rho_{X(p^k)}$, then the projection of ξ to $X(p^{k-O(k\delta)}) \times X(p^{k-O(k\delta)})$ lies on the Hecke curve T_d for some $d = p^{O(k\delta)}$.*

Proof. The proof in [BT16, Proposition 14] works with a very slight modification, so we include a sketch here. Setting $\xi := (x, y)$ and $\xi' := (x', y')$, we may assume $\xi = (\iota, g^{-1}\iota)$ (respectively, $(\varpi, g\varpi)$) for some $g \in G(p^k)$. Set $t := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (respectively, $t := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$). Since ξ is a Heegner CM point, g commutes with $\bar{t}$, hence is in the $\mathbb{Z}/p^k\mathbb{Z}$-span of $\{1, \bar{t}\}$. We then produce $M_x, M_y \in \mathrm{SL}_2(\mathbb{Z})$ whose entries are of size $p^{O(k\delta)}$ with $x' := \bar{M}_x x$ and $y' := g^{-1}\bar{M}_y x$. Let $F \subset M_2(\mathbb{Z})$ be the $\mathbb{Z}$-span of $\{1, t\}$, and note that it is a saturated submodule. We have a map

$$F \xrightarrow{f} M_2(\mathbb{Z}), \quad f(X) = [t, M_y^{-1} X M_x] \tag{A.1}$$

which is nonzero as in [BT16, Lemma 15]. The element g is in the kernel of f mod p^k and has unit determinant (so is in particular of additive order p^k). Let $B := \mathrm{Image}(f)$ and note that the obstruction to lifting g to $\ker(f)$ is its image in $\mathrm{Tor}_1^{\mathbb{Z}}(\mathrm{coker}(f), \mathbb{Z}/p^k\mathbb{Z}) \subset B/p^kB$. The torsion of the cokernel has size $p^{O(k\delta)}$, as therefore does $\mathrm{Tor}_1^{\mathbb{Z}}(\mathrm{coker}(f), \mathbb{Z}/p^k\mathbb{Z})$, so there is a (nonzero) element $D \in \ker(f)$ of size $p^{O(k\delta)}$ whose mod p^k reduction up to scale differs from g by an element which is annihilated by $p^{O(k\delta)}$, and in particular is a multiple of $p^{k-O(k\delta)}$. This implies the claim. □

For the next statement on multiplicities of CM points on $X(p^k) \times X(p^k)$, we recall the following notation from [BT16]: for a set S of closed points of a curve C, we let

$$\mathrm{mult}_S(C) := \sum_{x \in S} \mathrm{mult}_x(C).$$

We also denote by $a(r)$ the area of a 1-dimensional radius r hyperbolic ball, so with our normalization $a(r) = 4\pi \sinh^2(r/2)$.

Corollary A.6. *For any sufficiently small $\delta > 0$, any prime p, and any sufficiently large positive integer k, we have that for any non-Hecke curve C in $X(p^k) \times X(p^k)$,*

$$\mathrm{mult}_{\mathrm{CM}^+}(C) = O(p^{-k\delta} \mathrm{vol}(C)).$$

Proof. This is as in [BT16, Proposition 25]. For sufficiently small δ_0, we write $\mathrm{CM}^+ = S \sqcup T$ where T is the subset of Heegner CM points whose image under $\pi : X(p^k) \times X(p^k) \to X(p^{k(1-\delta_0)}) \times X(p^{k(1-\delta_0)})$ lie on a Hecke curve of degree $\leq p^{k\delta_0}$. By [BT16, Theorem 19], for δ_1 a sufficiently small multiple of δ_0,

$$\begin{aligned}
\mathrm{mult}_{\mathrm{CM}^+}(C) &\ll \frac{1}{a(\delta_1 \rho_{X(p^k)})} \sum_{\xi \in S} \mathrm{vol}\left(C \cap B(\xi, \delta_1 \rho_{X(p^k)})\right) + \sum_{d \leq p^{k\delta_0}} (C.\pi^* T_d) \\
&\ll \frac{\mathrm{vol}(C)}{a(\delta_1 \rho_{X(p^k)})} + \sum_{d \leq p^{k\delta_0}} (T_d^* \pi_* C.\Delta) \\
&\ll \frac{\mathrm{vol}(C)}{a(\delta_1 \rho_{X(p^k)})} + \frac{\mathrm{vol}(C)}{a(\rho_{X(p^{k(1-\delta_0)})}/2)} \sum_{d \leq p^{k\delta_0}} \deg T_d \\
&\ll \left(p^{-2k\delta_1} + p^{3k\delta_0} \cdot p^{-k(1-\delta_0)}\right) \mathrm{vol}(C).
\end{aligned}$$

Choosing δ_0, δ_1 to be appropriate multiples of δ, the claim is proven. □

Remark A.7. In [BT16, Proposition 14] and [BT16, Proposition 25], Heegner and anti-Heegner CM points are treated together. In the preparation of this appendix, the authors of [BT16] realized that this was in error; the argument in [BT16, Proposition 14] only holds for Heegner CM points, and one must provide a separate argument for anti-Heegner CM points as is done in [BT13], which treats the compact Shimura curve case. This will be handled in a forthcoming erratum [BT26] by Bakker–Tsimerman.

Modifying the argument of [BT26] in the same way, we obtain:

Corollary A.8. *For any sufficiently small $\delta > 0$, any prime p, and any sufficiently large positive integer k, we have that for any non-Hecke curve C in $X(p^k) \times X(p^k)$,*

$$\mathrm{mult}_{\mathrm{CM}^-}(C) = O(p^{-k\delta} \mathrm{vol}(C)).$$

A.2.3. *Repulsion of bicusps and multiplicities.*

Lemma A.9 (cf. [BT16, Proposition 17])**.** *For any sufficiently small $\delta > 0$, any prime p, and any sufficiently large positive integer k, we have the following. If $\xi \in X(p^k) \times X(p^k)$ is within $(1/2 + \delta)\rho_{X(p^k)}$ of at least three distinct singular bicusps, then all the singular bicusps within $(1/2 + \delta)\rho_{X(p^k)}$ of ξ project to the same Hecke curve T_d in $X(p^{k-O(k\delta)}) \times X(p^{k-O(k\delta)})$ for some $d = p^{O(k\delta)}$.*

Proof. Enumerate the set of singular bicusps $T = \{\zeta_j = (c_j, c_j')\}$ that are within $(1/2 + \delta)\rho_{X(p^k)}$ of ξ. The first paragraph of the proof in [BT16] shows that for any two distinct ζ_j, ζ_k, both projections to $X(p^k)$ must be distinct, and that we may assume $\xi = (\iota, g\iota)$

for $g \in G(p^k)$. For each j we produce $M_j, M_j' \in \mathrm{SL}_2(\mathbb{Z})$ of size $p^{O(k\delta)}$ with $c = \bar{M}_j\mathfrak{y}$ and $c_j' = g\bar{M}_j'\mathfrak{y}$, and the argument of case (1) shows that the cosets $\bar{M}_j N(\bar{H})$ are pairwise distinct, as are the cosets $\bar{M}_j' N(\bar{H})$. We have that $g \in \bigcap_j \bar{M}_j N(\bar{H}) \bar{M}_j'^{-1} \subset G(p^k)$. Consider the map

$$M_2(\mathbb{Z}) \xrightarrow{f} \mathbb{Z}^T, \quad f(X)_j = \text{lower left entry of } M_j^{-1} X M_j' \tag{A.2}$$

whose cokernel has size $p^{O(k\delta)}$. Since $|T| \geq 3$, $\ker(f)$ is at most rank one given that any $X \in \ker(f)$ fixes at least 3 points on $\mathbb{P}^1(\mathbb{R})$. As before, g is an element of the kernel mod p^k of additive order p^k, so there exists an element $D \in \ker(f)$ of height $p^{O(k\delta)}$ whose reduction up to scale agrees with g mod $p^{k-O(k\delta)}$.

□

Corollary A.10. *For any sufficiently small $\delta > 0$, any prime p, and any sufficiently large positive integer k, we have that for any non-Hecke curve C in $X(p^k) \times X(p^k)$,*

$$p^k \cdot \mathrm{mult}_{\mathrm{SBC}}(C) = O(p^{-k\delta} \operatorname{vol}(C)).$$

Proof. The proof is as in [BT16, Proposition 26] (with the correction from [BT26]) and the above corollary. We leave the details to the reader. Note that the proof of [BT16, Proposition 12] does not use that p is prime. □

A.3. **Proving Theorem A.1.** Because we are working in terms of the genus of our function field rather than the gonality, we can side-step the arguments involving the symmetric product from the strategy outlined above and hence bypass having to generalize the results on multidiagonals from [BT16]. The argument therefore runs parallel to that of [BT13]—see [BT16, p. 711] for related comments.

By the discussion in Section A.1, Theorem A.1 is equivalent to the following statement, which we now prove.

Theorem A.11. *Let g be a non-negative integer. There exists a positive integer $\mathcal{N}(g)$ such that, for all prime powers p^k, if $C \to Z(p^k)$ is a non-Hecke curve of genus g, then $p^k \leq \mathcal{N}(g)$.*

Proof. First, note that it suffices to prove the statement for prime powers $N = p^k$. Fix $g \in \mathbb{Z}^+$ and suppose to the contrary that for arbitrarily large prime powers p^k we have a non-Hecke curve $C \to Z(p^k)$ of genus g. For any sufficiently large prime power p^k, we take the normalization C' of a component of the lift of C with respect to the quotient map $q : X(p^k) \times X(p^k) \to Z(p^k)$.

$$\begin{array}{ccc} C' & \xrightarrow{\psi} & X(p^k) \times X(p^k) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle q} \\ C & \longrightarrow & Z(p^k) \end{array}$$

The ramification of α is supported on that of the map q, and hence occurs only at points in the fibers under ψ over CM points and singular bicusps. The ramification index of $\psi^{-1}(\xi)$ for any $\xi \in \mathrm{SBC}$ is $O(p^k)$, while that for $\xi \in \mathrm{CM}$ is at most 3. By Corollary A.6, Corollary A.8, and Corollary A.10, we then have

$$\mathrm{Ram}(\alpha) \ll |\psi^{-1}(\mathrm{CM})| + p^k \cdot |\psi^{-1}(\mathrm{SBC})| = o(\mathrm{vol}(C')).$$

Riemann–Hurwitz then gives

$$g(C') = O(\deg(\alpha)) + o(\mathrm{vol}(C')), \tag{A.3}$$

where the implied constant in the first term depends on g. On the other hand, by the Schwarz lemma we have $g(C') \gg \mathrm{vol}(C')$, so

$$\mathrm{vol}(C') = O(\deg(\alpha)).$$

Letting $\deg_{X(p^k)}(C')$ be the maximum degree of the projections $C' \to X(p^k)$, we see that $\mathrm{vol}(C')$ is comparable to $\deg_{X(p^k)}(C') \cdot \mathrm{vol}(X(p^k))$, which is in turn comparable to $\deg_{X(p^k)}(C') \cdot |G(p^k)|$ (since $-\chi(X(1)_{p^k}) = \frac{1}{6} - p^{-k}$). Thus, $\deg_{X(p^k)}(C')$ is bounded. From the commutative square

$$\begin{array}{ccc} C' & \longrightarrow & X(p^k) \\ \downarrow{\scriptstyle \alpha} & & \downarrow \\ C & \longrightarrow & X(1)_{p^k} \end{array}$$

we deduce $\deg_{X(1)_{p^k}}(C)$ is bounded. As in [BT13, §5], there is a bounded family of such curves $C \to X(1)_{p^k} \times X(1)_{p^k}$, and therefore finitely many possibilities for the image on fundamental groups (after removing the cusps). For any non-Hecke curve, this image is Zariski dense in $\mathrm{SL}_2 \times \mathrm{SL}_2$ by André–Deligne [And92], and using [Rap14, Lemma 2.7] in place of the theorem of Nori we have a contradiction. □

References

[And92] Yves André. Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part. *Compositio Math.*, 82(1):1–24, 1992.

[BLV09] Andrea Bandini, Ignazio Longhi, and Stefano Vigni. Torsion points on elliptic curves over function fields and a theorem of Igusa. *Expo. Math.*, 27(3):175–209, 2009.

[BT13] B. Bakker and J. Tsimerman. On the Frey-Mazur conjecture over low genus curves. arXiv:1309.6568, 2013.

[BT16] Benjamin Bakker and Jacob Tsimerman. p-torsion monodromy representations of elliptic curves over geometric function fields. *Ann. of Math. (2)*, 184(3):709–744, 2016.

[BT26] B. Bakker and J. Tsimerman. Erratum to "p-torsion monodromy representations of elliptic curves over geometric function fields". https://benjamin-bakker.github.io/P.torsion.erratum.pdf, 2026.

[CH05] Alina Carmen Cojocaru and Chris Hall. Uniform results for Serre's theorem for elliptic curves. *Int. Math. Res. Not.*, (50):3065–3080, 2005.

[Coj05] Alina Carmen Cojocaru. On the surjectivity of the Galois representations associated to non-CM elliptic curves. *Canad. Math. Bull.*, 48(1):16–31, 2005. With an appendix by Ernst Kani.

[EvdGM] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. *Abelian Varieties*.

[Fis14] Tom Fisher. On families of 7- and 11-congruent elliptic curves. *LMS J. Comput. Math.*, 17(1):536–564, 2014.

[FK22] Nuno Freitas and Alain Kraus. On the symplectic type of isomorphisms of the p-torsion of elliptic curves. *Mem. Amer. Math. Soc.*, 277(1361):v+105, 2022.

[Fre24] Sam Frengley. On 12-congruences of elliptic curves. *Int. J. Number Theory*, 20(2):565–601, 2024.

[GP22] Richard Griffon and Fabien Pazuki. Isogenies of elliptic curves over function fields. *Int. Math. Res. Not. IMRN*, (19):14697–14740, 2022.

[Igu59] Jun-ichi Igusa. Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves. *Amer. J. Math.*, 81:453–476, 1959.

[LF16] Samuel Le Fourn. Surjectivity of Galois representations associated with quadratic $\mathbb{Q}$-curves. *Math. Ann.*, 365(1-2):173–214, 2016.

[Lom15] Davide Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra Number Theory*, 9(10):2347–2395, 2015.

[Lom16a] Davide Lombardo. An explicit open image theorem for products of elliptic curves. *J. Number Theory*, 168:386–412, 2016.

[Lom16b] Davide Lombardo. Explicit surjectivity of Galois representations for abelian surfaces and GL_2-varieties. *J. Algebra*, 460:26–59, 2016.

[LV14] Eric Larson and Dmitry Vaintrob. On the surjectivity of Galois representations associated to elliptic curves over number fields. *Bull. Lond. Math. Soc.*, 46(1):197–209, 2014.

[Mil86] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[Mum08] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[MW93a] D. W. Masser and G. Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3):247–254, 1993.

[MW93b] David Masser and Gisbert Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

[MW24] Jacob Mayle and Tian Wang. On the effective version of Serre's open image theorem. *Bull. Lond. Math. Soc.*, 56(4):1399–1416, 2024.

[MW25] Jacob Mayle and Tian Wang. An effective open image theorem for products of principally polarized abelian varieties. *J. Number Theory*, 274:140–179, 2025.

[Rap14] Andrei S. Rapinchuk. Strong approximation for algebraic groups. In *Thin groups and superstrong approximation*, volume 61 of *Math. Sci. Res. Inst. Publ.*, pages 269–298. Cambridge Univ. Press, Cambridge, 2014.

[Rib76] Kenneth A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[Ros86] Michael Rosen. Abelian varieties over $\mathbf{C}$. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 79–101. Springer, New York, 1986.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[Zyw22] David Zywina. On the surjectivity of mod ℓ representations associated to elliptic curves. *Bull. Lond. Math. Soc.*, 54(6):2404–2417, 2022.

Benjamin Bakker

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA

URL: https://benjamin-bakker.github.io
Email address: bakker@gmail.com

Alina Carmen Cojocaru

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA
- Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania

URL: https://www.alinacarmencojocaru.com/
Email address: math.cojocaru@gmail.com

Frederick Saia

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA

URL: https://fsaia.github.io/site/
Email address: freddy.v.saia@gmail.com