Explicit descent on elliptic curves and splitting Brauer classes

Benjamin Antieau and Asher Auel

July 21, 2021

Abstract

We prove new results on splitting Brauer classes by genus 1 curves, settling in particular the case of index 7 classes over global fields. Though our method is cohomological in nature, and proceeds by considering the more difficult problem of splitting μ_N-gerbes, we use crucial input from the arithmetic of modular curves and explicit N-descent on elliptic curves.

1 Introduction

Inspired by work of Artin [2] on Severi–Brauer varieties, Pete Clark [13] and David Saltman [54] have asked whether, given a Brauer class $\alpha \in \mathrm{Br}(k)$ over a field k, there exists a (smooth proper geometrically irreducible) genus 1 curve C/k such that α is split by C. By 'split' we mean that α pulls back to zero in $\mathrm{Br}(C)$, or equivalently, in $\mathrm{Br}(k(C))$. We remark that if a curve of genus g splits α, then the index of α must divide $2g-2$, showing the relevance of the genus 1 hypothesis.

Work of Swets [62] handles the case when α has index $\leqslant 3$, de Jong and Ho [16] settle the case when α has index $\leqslant 5$, and the case of index 6 is indicated in [3]. In a slightly different direction, Roquette [53], Lichtenbaum [32], Ciperiani and Krashen [11], and Krashen and Lieblich [30] give results and algorithms to compute the kernel of $\mathrm{Br}(k) \to \mathrm{Br}(C)$ when C is a fixed genus 1 curve. Using these results, one can establish an affirmative answer to the question when k is a local field: see Example 2.4. However, the question is still wide open, notably over global fields. One of our main contributions is the following.

Theorem. *Every Brauer class α of index 7 over a global field k is split by a genus 1 curve.*

In fact, we prove much more by considering a strengthening of the question: given a class $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$, is there a genus 1 curve C/k such that β is split by C? Here, by 'split' we mean that β pulls back to zero in $\mathrm{H}^2(C, \mu_N)$, and to emphasize this, we say that C splits the μ_N-gerbe β. Note that this is not equivalent to β pulling back to zero in $\mathrm{H}^2(\operatorname{Spec} k(C), \mu_N)$. Indeed, if β is split by C, then the image $\alpha \in \mathrm{Br}(k)$ under the isomorphism $\mathrm{H}^2(\operatorname{Spec} k, \mu_N) \cong \mathrm{Br}(k)[N]$, is split by C, but the converse is not generally true. Unless otherwise specified, cohomology groups are taken with respect to the fppf topology.

For example, using the Tate pairing, one can show that if k is a non-archimedean local field and $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N) \cong \mathbf{Z}/N$, then β is split by a genus 1 curve; see Proposition 3.9.

In our main theorem, we mention cyclic classes, i.e., those in the image of the cup product map $(\chi, u) \mapsto \chi \cup u$ in cohomology $\mathrm{H}^1(\operatorname{Spec} k, \mathbf{Z}/N) \times \mathrm{H}^1(\operatorname{Spec} k, \mu_N) \to \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$. The theorem of Albert, Brauer, Hasse, and Noether says that if k is a global field, then every class of $\mathrm{H}^2(\operatorname{Spec} k, \mu_N)$ is cyclic. This fact is central to the proof of the following.

Theorem A. *Let k be a field and $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$. Then the μ_N-gerbe β is split by a genus 1 curve in the following cases:*

- $N = 2, 3, 4, 5$ *and* β *is cyclic,*
- $N = 6, 7, 10$ *and* k *is a global field,*
- $N = 8$, k *is a global field, and either* $\operatorname{char}(k) = 2$ *or* k *contains a primitive* 8*th root of unity,*
- $N = 9$, k *is a global field, and either* $\operatorname{char}(k) = 3$ *or* k *contains* $\zeta_9 + \zeta_9^{-1}$ *for a primitive* 9*th root of unity* ζ_9*, or*
- $N = 12$, k *is a global field, and either* $\operatorname{char}(k) = 2$ *or* k *contains a primitive* 4*th root of unity.*

The reader will observe that the N appearing in Theorem A are precisely those for which the modular curve $X_1(N)$ has genus 0 (see for example [46]). This is not a coincidence; the proof uses explicit 1-parameter families of elliptic curves with exact order N points constructed using Tate normal form; see the work of Kubert [31] and the reference by Knapp [27, V.5] as well as the tables by Sutherland [61, 60]. `MAGMA` [9] code provided by Tom Fisher allows us to do explicit μ_N-descent on these curves, which we do to generate lots of classes β split by genus 1 curves. Saltman led us to the cyclicity theorem of Albert [1], generalized to non-prime-degree algebras by Vishne [68] and Mináč–Wadsworth [43], which allows us to prove that in the global cases these classes span the entire group $\mathrm{H}^2(\operatorname{Spec} k, \mu_N)$ under the assumptions in the theorem.

While our results for splitting μ_N-gerbes, covering small N and particular fields k, might seem limited, there is little chance that they can be improved in general. Indeed, over $\mathbf{Q}$, no μ_p-gerbe is split by a genus 1 curve if $p \geqslant 11$ is a prime (see Example 3.8), although the question of whether classes in $\operatorname{Br}(\mathbf{Q})[p]$ are split by genus 1 curves is still open. Additionally, we remark that the splitting problem for μ_N-gerbes is sensitive to N: in Example 3.7, we give an example of an index 2 Brauer class α split by a genus 1 curve X, where X splits the unique lift of α to $\mathrm{H}^2(\operatorname{Spec} k, \mu_4)$ but does not split the unique lift to $\mathrm{H}^2(\operatorname{Spec} k, \mu_2)$.

As an additional illustration of our methods, we also prove that every class $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$ is split by a torsor for an abelian variety; see Section 3.3. This gives a new proof of the fact that every Brauer class is split by an abelian variety torsor, which was first proved by Ho and Lieblich in [23]. They prove even more, namely that every Brauer class is split by a torsor for the Jacobian of a curve, typically of very high genus. The curves they employ have simple Jacobians and they wonder whether one can split Brauer classes by products of genus one curves. We use our methods to address this question in many cases in Theorem B and C.

Theorem B. *Let* k *be a field and let* $N \geqslant 2$ *be an integer invertible in* k*. If* $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$*, then the* μ_N*-gerbe* β *is split by a product of genus* 1 *curves in the following cases:*

- $N = 2, 3, 5, 6, 10, 15, 30$ *or*
- $N = 4, 12, 20, 60$ *if* k *contains a primitive* 4*th root of unity.*

Clark first suggested in unpublished work [13] a close connection between the splitting problem and the period-index obstruction map for genus 1 curves studied by O'Neil [48] and Clark [12]. We use those ideas to prove the following theorem, clarifying along the way the relationship between the period-index map and the cup product. The theorem applies to cyclic Brauer classes, i.e., the Brauer classes associated to cyclic μ_N-cohomology classes.

Theorem C. *Let* k *be a field and fix an elliptic curve* E *over* k *with a full level* N *structure* $E[N] \cong \mathbf{Z}/N \times \mu_N$*. If* $\alpha \in \operatorname{Br}(k)[N]$ *is cyclic, then* α *is split by an* E*-torsor.*

Saltman [55, Corollary 2] has given another proof of the $N = 3$ case of Theorem C, and also gives examples to show that there are obstructions to splitting cubic classes by genus 1 curves with Jacobians of given j-invariant.

It is always possible to arrange for the existence of an elliptic curve with a full level N structure as above after a small Galois extension of k. So, we obtain our main corollary, which says that, after some small extensions, we can split arbitrary Brauer classes by products of genus 1 curves while controlling the j-invariants of their Jacobians. Note that in the contexts of Theorems A and B, there is no control of the j-invariants of the Jacobians.

Corollary D. *Let k be a field and let $N > 1$ be an integer. Fix an elliptic curve E over k, which is non-supersingular if the characteristic of k divides N. There is a finite extension K over k of degree dividing the order of $\mathrm{GL}_2(\mathbf{Z}/N)$ such that every $\alpha \in \mathrm{Br}(K)[N]$ is split by a product of E-torsors.*

The extension K is obtained by adjoining the coordinates of the N-torsion points of E, with suitable modifications if the characteristic divides N. The number of torsors needed to split β or α in Theorems B and Corollary D is dictated by the symbol lengths of β or α when expressed as sums of cyclic classes using the theorems of Teichmüller (when k has characteristic p and N is a p-power, see [20, Thm. 9.1.4]), Merkurjev [38, 39] ($N = 2, 3$), Matzri [36] ($N = 5$), and Merkurjev–Suslin [40] (when N is invertible in k, noting that the extension K in Corollary D will contain a primitive Nth root of unity).

We mention a series of examples where Theorem C and Corollary D can be applied.

Example I. In the setting of Hilbert's 12th problem (Kronecker's Jugendtraum), suppose that k is an imaginary quadratic number field k with class number 1 and E is an elliptic curve over k with complex multiplication in k. If $K = k^{\mathrm{ab}} = k(E_{\mathrm{tors}}(\overline{k}))$ is the maximal abelian extension (see [58, Chap. II]) obtained by adjoining the coordinates of the torsion points of E, then every cyclic algebra over any field L containing K is split by an E-torsor and every Brauer class over any such field L is split by a product of E-torsors.

Example II. If E is any elliptic curve defined over $\overline{\mathbf{Q}}$, then every cyclic algebra over any field L containing $\overline{\mathbf{Q}}$ is split by an E-torsor and every Brauer class over any such field L is split by a product of E-torsors. This gives examples of the phenomenon with arbitrary algebraic j-invariant.

Example III. In characteristic p, no extension is necessary when $N = p$. By a theorem of Deuring [17], also called the Hasse–Deuring–Waterhouse theorem (see [71]), there is an elliptic curve E over $\mathbf{F}_p$ with exactly p rational points. In particular, it is ordinary and admits a full level p structure. This fact can also be seen by the more general Honda–Tate theory [64, 24, 66]; the elliptic curve corresponds to the Weil polynomial $T^2 - T + p$ and is unique up to isogeny. Therefore, for any field k of characteristic p, every cyclic class of $\mathrm{Br}(k)[p]$ is split by an E-torsor, and by the above mentioned theorem of Teichmüller (see [20, Thm. 9.1.4]), every class of $\mathrm{Br}(k)[p]$ is a sum of cyclic algebras and hence is split by a product of E-torsors.

Example IV. If E is any ordinary elliptic curve defined over $\overline{\mathbf{F}}_p$, then E admits a full level N structure for any N. Therefore, for any field L containing $\overline{\mathbf{F}}_p$, every cyclic class in $\mathrm{Br}(L)$ is split by an E-torsor. However, by a theorem of Albert (see [20, Thm. 9.1.8]), every class in $\mathrm{Br}(k)[p^\infty]$ is cyclic. This proves that any p-primary Brauer class over a field containing $\overline{\mathbf{F}}_p$ is split by a genus 1 curve.

Finally, we provide two additional applications of our methods to splitting Galois cohomology classes of higher degree by products of genus one curves.

Corollary E. *Let k be a field, let $N \mid 60$ and assume that k contains a primitive Nth root of unity. For any degree $n \geqslant 2$, any $\beta \in \mathrm{H}^n(\operatorname{Spec} k, \mu_N)$ is split by a product of genus 1 curves. The same result holds for N-torsion classes of $\mathrm{H}^n(\operatorname{Spec} k, \mathbf{G}_m)$.*

Proof. By the Bloch–Kato conjecture, we can write $\beta = \beta_1 + \cdots + \beta_d$ as a sum of d symbols $\beta_i = u_{i1} \cup \cdots \cup u_{in}$, where each $u_{ij} \in k^\times/(k^\times)^N$, and where we use a primitive Nth root of unity to give an isomorphism $\mathbf{Z}/N \cong \mu_N$. Each $u_{i1} \cup u_{i2} \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$ can be split by a product of genus 1 curves by Theorem B. But, this implies that each β_i is split by a product of genus 1 curves and hence so is β. □

Splitting higher degree Galois cohomology classes, combined with the Milnor conjecture for the Witt group as proved by Voevodsky [69], [70] and Orlov–Vishik–Voevodsky [50], we arrive at the following application to the study of Witt kernels for torsors under abelian varieties.

Corollary F. *Let σ be a quadratic form of even dimension $d \geqslant 4$ and trivial discriminant over a field k of characteristic $\neq 2$. Then, σ becomes hyperbolic after extension to the function field of a product of genus 1 curves.*

Proof. A consequence of the Arason–Pfister Hauptsatz and the Milnor conjectures for the Witt group is the statement that a quadratic form σ is hyperbolic if and only if $e_n(\sigma) = 0$ for all $n \geqslant 0$, where $e_n : I^n(k) \to \mathrm{H}^n(k, \mu_2)$ are the higher cohomological invariants on the fundamental filtration of the Witt group, see [18, Sections 16, 23.A]. By successively splitting $e_n(\sigma)$ and then subtracting off a sum of Pfister forms representing $e_n(\sigma)$, it follows that σ will become hyperbolic over any field extension that splits a certain finite collection of mod 2 Galois cohomology classes. The hypotheses on σ imply that $e_0(\sigma) = e_1(\sigma) = 0$, and then Corollary E applies to show that we can split any finite collection of Galois cohomology classes of degree $\geqslant 2$ by a product of genus 1 curves. □

We remark that the conditions on the dimension and discriminant are necessary. Whether a quadratic form in $I^2(k)$ becomes hyperbolic over the function field of a genus 1 curve is an open question.

Outline. Section 2 mostly contains background on the cohomological pairings that will be important for our work, emphasizing their stack-theoretic development and interpretation. Readers very well-acquainted with the Weil and Tate pairings could reasonably skip Sections 2.1 and 2.2, but should look at Section 2.4 on the period-index obstruction theory for genus 1 curves, which contains the main tools going into proving Theorem C. Section 3 sets up the general problem of splitting μ_N-gerbes and contains proofs of the main theorems. In particular, Section 3.1 includes many examples showing the difference between the problem of splitting Brauer classes and splitting μ_N-gerbes, as well as complete solutions over nonarchimedean local fields and the real numbers, while Section 3.2 explains the relationship between N-isogenies and splitting genus μ_N-gerbes. Finally, Appendix A contains the explicit descent calculations we use in the proof of Theorem A.

Acknowledgments. We benefited from conversations with Pete Clark, Skip Garibaldi, David Gepner, Danny Krashen, Max Lieblich, Lennart Meier, Anthony Várilly-Alvarado, Bianca Viray, and John Voight and we thank them for their insights. Special thanks go to Tom Fisher who provided `MAGMA` code and David Saltman for a pivotal observation. Finally, Pete Clark, Cathy O'Neil, David Saltman, and John Voight gave us invaluable feedback and pointers on a preliminary version of this paper.

BA was supported by the NSF under grants DMS-2102010 and DMS-2120005 and by a Simons Fellowship. He would like to thank the departments at Dartmouth and Yale for their hospitality during visits where this work was carried out. AA was supported by a Simons Foundation Collaboration Grant and a Walter and Constance Burke Research Award.

Work on this project began at the workshop "The use of linear algebraic groups in geometry and number theory" at Banff in September 2015. We thank the organizers, Garibaldi, Lemire, Parimala, and Zainoulline, for creating the occasion and BIRS for providing a wonderful setting for research.

2 Cohomology and pairings

We give some background on the Tate and Weil pairings, cyclic algebras, and the O'Neil period-index obstruction map [48]. This work culminates in Proposition 2.13, which gives the connection between the period-index obstruction map and cyclic algebras, generalizing prior work of O'Neil [48] and Clark [12].

2.1 The Tate pairing

Mumford attributes the following statement to Rosenlicht and Serre; see [45, p. 227]. Let S be an arbitrary base scheme.

Proposition 2.1 (Rosenlicht–Serre)**.** *Let $p\colon A \to S$ be an abelian scheme. The fppf Ext sheaf $\mathscr{E}xt^1(A, \mathbf{G}_m)$ is naturally isomorphic to the dual abelian scheme $\widehat{A} = \mathrm{Pic}^0_{A/S}$, while*

$$\mathscr{E}xt^0(A, \mathbf{G}_m) = 0.$$

Proof. We use a technique from crystalline cohomology, namely a resolution

$$\cdots \to \mathbf{Z}[A^3] \oplus \mathbf{Z}[A^2] \to \mathbf{Z}[A^2] \to \mathbf{Z}[A] \to A$$

in fppf sheaves of abelian groups (see [6] for details). We will only need that the homomorphism $\mathbf{Z}[A^2] \to \mathbf{Z}[A]$ is given by $m^* - p_1^* - p_2^*$, where $m : A^2 \to A$ is the group law on A and $p_i : A^2 \to A$ are the projections. Taking Ext sheaves out of this resolution into $\mathbf{G}_m$, we obtain a spectral sequence converging to $\mathscr{E}xt^*(A, \mathbf{G}_m)$. Because each term A^n appearing is proper and geometrically connected, the 0-line given by $\mathscr{E}xt^0(\mathbf{Z}[A^n], \mathbf{G}_m) \cong \mathrm{R}^0 p_* \mathbf{G}_m$ is $\mathbf{G}_m \xrightarrow{\mathrm{id}} \mathbf{G}_m \to \mathbf{G}_m \times \mathbf{G}_m \to \cdots$. The 1-line is given by $\mathrm{R}^1 p_* \mathbf{G}_m$ from the various copies of A, which gives $\mathrm{Pic}_{A/S} \to \mathrm{Pic}_{A^2/S} \to \cdots$. Hence, we see that $\mathscr{E}xt^0(A, \mathbf{G}_m) = 0$ and that $\mathscr{E}xt^1(A, \mathbf{G}_m)$ is given by the kernel of the map

$$\mathrm{Pic}_{A/S} \xrightarrow{\mathcal{L} \mapsto m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1}} \mathrm{Pic}_{A^2/S}\,.$$

It is part of the construction of the dual abelian variety, cf. [45, §13], that this kernel is the connected component $\widehat{A} = \mathrm{Pic}^0_{A/S}$ of the identity. □

For any n, the Yoneda product (composition) induces a bilinear pairing

$$\widehat{A} \times \mathrm{B}^n A \to \mathrm{B}^{n+1} \mathbf{G}_m$$

of commutative group stacks. When $n = 0$, we obtain $\widehat{A} \times A \to \mathrm{B}\mathbf{G}_m$, which classifies the Poincaré line bundle (cf. [25, Theorem 9.14]), while for $n = 1$ we obtain $\widehat{A} \times \mathrm{B}A \to \mathrm{B}^2\mathbf{G}_m$, which defines the bilinear Tate pairing.

Definition 2.2. The **Tate pairing** will refer to the bilinear pairing on cohomology

$$[-,-]_T\colon \widehat{A}(S) \times \mathrm{H}^1(S, A) \to \mathrm{H}^2(S, \mathbf{G}_m)$$

induced from $\widehat{A} \times \mathrm{B}A \to \mathrm{B}^2\mathbf{G}_m$ as above.

Here are two different perspectives on the Tate pairing, cf. [11, Thm. 3.7] and the citations there. The following interpretations of the Tate pairing can also be easily deduced from the functoriality of the Yoneda product and $\mathscr{E}xt^*$.

First, there is the semiabelian point of view. Sections $\mathcal{L}$ of $\widehat{A} \cong \mathscr{E}xt^1(A, \mathbf{G}_m)$ classify semiabelian S-scheme extensions $A_{\mathcal{L}}$ of the form

$$1 \to \mathbf{G}_m \to A_{\mathcal{L}} \to A \to 0.$$

Pairing with $\mathcal{L}$ induces a homomorphism that on S-points corresponds to the boundary maps

$$[\mathcal{L}, -]_T\colon \mathrm{H}^n(S, A) \to \mathrm{H}^{n+1}(S, \mathbf{G}_m),$$

in the long exact sequence associated to the extension $A_{\mathcal{L}}$. Thus, if $X \in \mathrm{H}^1(S, A)$, then the class $[\mathcal{L}, X]_T \in \mathrm{H}^2(S, \mathbf{G}_m)$ is the obstruction to lifting the A-torsor X to an $A_{\mathcal{L}}$-torsor.

Second, there is the Leray–Serre point of view. Fixing an A-torsor X, the connected component $\mathrm{Pic}^0_{X/S}$ of the identity of $\mathrm{Pic}_{X/S}$ is isomorphic to $\widehat{A}$. The Leray–Serre spectral sequence

$$\mathrm{E}_2^{s,t} = \mathrm{H}^s(S, \mathrm{R}^t p_* \mathbf{G}_m) \Longrightarrow \mathrm{H}^{s+t}(X, \mathbf{G}_m)$$

has a d_2-differential giving a homomorphism

$$d_2^X \colon \mathrm{Pic}_{X/S}(S) \cong \mathrm{H}^1(S, \mathrm{R}^1 p_* \mathbf{G}_m) \to \mathrm{H}^2(S, \mathrm{R}^0 p_* \mathbf{G}_m) \cong \mathrm{H}^2(S, \mathbf{G}_m).$$

When restricted to $\mathcal{L} \in \mathrm{Pic}^0_{X/S}(S)$, we have $[\mathcal{L}, X]_T = d_2^X(\mathcal{L})$. When $S = \operatorname{Spec} k$ is the spectrum of a field, this differential is the obstruction to lifting the Galois-invariant divisor class $\mathcal{L} \in \mathrm{Pic}^0_{X/k}(S)$ to a line bundle on X.

The relevance of the Tate pairing to the problem of splitting Brauer classes by torsors under abelian schemes stems from the fact that, according to the Leray–Serre perspective, an A-torsor X splits any class of the form $[\mathcal{L}, X]_T \in \mathrm{H}^2(S, \mathbf{G}_m)$, cf. [11, Section 3.1].

We illustrate how to use the Tate pairing to show that every Brauer class on a local field is split by a genus 1 curve.

Theorem 2.3 (Tate [63], Shatz [57], Milne [41, 42])**.** *If K is a non-archimedean local field and we equip $\widehat{A}(K)$ with the analytic topology and $\mathrm{H}^1(\operatorname{Spec} K, A)$ with the discrete topology, then the Tate pairing*

$$[-,-]_T \colon \widehat{A}(K) \times \mathrm{H}^1(\operatorname{Spec} K, A) \to \mathrm{Br}(K) \cong \mathbf{Q}/\mathbf{Z}$$

is continuous and non-degenerate.

Example 2.4. Let K be a non-archimedean local field with uniformizer ϖ. The elliptic curve E over $\operatorname{Spec} K$ given by $y^2 + xy = x^3 + \varpi^N$ has split multiplicative reduction and, by a result of Kodaira and Néron (see [59, Thm. VII.6.1] or [8, Sec. 1.5]), $E(K)/E_0(K) \cong \mathbf{Z}/N$, where $E_0(K) \subseteq E(K)$ is the group of points of smooth reduction. It follows from the non-degeneracy of the Tate pairing that, for any generator P of $E(K)/E_0(K)$, there exists an E-torsor X such that $[P, X]_T$ generates $\frac{1}{N}\mathbf{Z}/\mathbf{Z} \subseteq \mathbf{Q}/\mathbf{Z}$.[1] In particular, every class of $\mathrm{Br}(K) \cong \mathbf{Q}/\mathbf{Z}$ is split by a genus 1 curve.

2.2 The Weil pairing

Let $\varphi \colon A \to A'$ be an isogeny of abelian S-schemes with kernel $\ker(\varphi)$. Taking $\mathscr{E}xt^*$ into $\mathbf{G}_m$, we obtain an exact sequence

$$0 \to \mathscr{E}xt^0(\ker(\varphi), \mathbf{G}_m) \to \mathscr{E}xt^1(A', \mathbf{G}_m) \to \mathscr{E}xt^1(A, \mathbf{G}_m) \to \mathscr{E}xt^1(\ker(\phi), \mathbf{G}_m).$$

The central two terms can be rewritten as $\widehat{A'} \xrightarrow{\widehat{\varphi}} \widehat{A}$, which is the dual isogeny. Since isogenies are surjective as fppf sheaves, we obtain a short exact sequence

$$0 \to \widehat{\ker(\varphi)} \to \widehat{A'} \xrightarrow{\widehat{\varphi}} \widehat{A} \to 0,$$

where $\widehat{\ker(\varphi)}$ is the usual Cartier dual. In particular, we obtain a canonical isomorphism between the Cartier dual of $\ker(\varphi)$ and of $\ker(\widehat{\varphi})$. In other words, there is a canonical perfect pairing

$$\ker(\varphi) \times \ker(\widehat{\varphi}) \to \mathbf{G}_m.$$

If $\ker(\varphi) \subseteq A[N]$, e.g., if φ is an N-isogeny, then this pairing lands in μ_N.

[1] Here and elsewhere we will silently identify E with $\widehat{E}$ via the polarization arising from the ample line bundle $\mathcal{O}(0_E)$.

Example 2.5. If φ is multiplication by N, we obtain the Weil pairing

$$A[N] \times \widehat{A}[N] \to \mu_N.$$

In the special case of an elliptic curve E (or a principally polarized abelian variety), we can rewrite this as a perfect pairing $E[N] \times E[N] \to \mu_N$.

Definition 2.6. While there are several possible versions of a **cohomological Weil pairing**, we will need the following two on an elliptic curve E over S. If φ is an N-isogeny, then the Weil pairing associated to φ is the bilinear pairing

$$(-,-)_\varphi \colon \mathrm{H}^1(S, \ker(\varphi)) \times \mathrm{H}^1(S, \ker(\widehat{\varphi})) \to \mathrm{H}^2(S, \mu_N)$$

taking values in μ_N-cohomology. Taking multiplication by N, the Weil pairing is the bilinear pairing

$$[-,-]_N \colon \mathrm{H}^1(S, E[N]) \times \mathrm{H}^1(S, E[N]) \to \mathrm{H}^2(S, \mathbf{G}_m)$$

taking values in the Brauer group.

Remark 2.7. The following compatibility between the Tate and Weil pairings will be useful to us. Suppose that $X \in \mathrm{H}^1(S, E)[N]$, i.e, an N-torsion element of $\mathrm{H}^1(S, E)$. Pairing with X defines a homomorphism $[-, X]_T \colon E(S) \to \mathrm{H}^2(S, \mathbf{G}_m)$ that factors through $E(S)/NE(S) \subseteq \mathrm{H}^1(S, E[N])$. If we lift X to an $E[N]$-torsor Y, then we have that for $\mathcal{L} \in E(S)$

$$[\mathcal{L}, X]_T = [\overline{\mathcal{L}}, Y]_N$$

in $\mathrm{H}^2(S, \mathbf{G}_m)$, where $\overline{\mathcal{L}}$ is the image of $\mathcal{L}$ in $E(S)/NE(S)$.

2.3 The cup product pairing and cyclic algebras

The groups $\mathbf{Z}/N$ and μ_N are Cartier dual. Under the natural identification $\mu_N = \mathscr{H}om(\mathbf{Z}/N, \mathbf{G}_m)$, the bilinear evaluation pairing $\mathbf{Z}/N \times \mu_N \to \mathbf{G}_m$ takes the form $(a, \zeta) \mapsto \zeta^a$, hence takes values in μ_N. It induces a canonical isomorphism of sheaves $\mathbf{Z}/N \otimes \mu_N \cong \mu_N$. Thus we have a bilinear cup product pairing

$$(-) \cup (-) \colon \mathrm{H}^1(S, \mathbf{Z}/N) \times \mathrm{H}^1(S, \mu_N) \to \mathrm{H}^2(S, \mathbf{Z}/N \otimes \mu_N) \to \mathrm{H}^2(S, \mu_N)$$

and classes of the form $\chi \cup u$ in $\mathrm{H}^2(S, \mu_N)$ are called cyclic.[2]

This pairing is related to the cyclic algebra construction as follows. Consider the nontoral embedding $\mathbf{Z}/N \times \mu_N \hookrightarrow \mathrm{PGL}_N$, which on points sends $(1, 1)$ to the $N \times N$-matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

and $(0, \zeta)$ to the diagonal matrix $(1, \zeta, \ldots, \zeta^{N-1})$. This embedding induces a map on cohomology

$$\mathrm{H}^1(S, \mathbf{Z}/N \times \mu_N) = \mathrm{H}^1(S, \mathbf{Z}/N) \times \mathrm{H}^1(S, \mu_N) \to \mathrm{H}^1(S, \mathrm{PGL}_N)$$

[2]Note that we write u for a general element of $\mathrm{H}^1(S, \mu_N)$, although for a general scheme u is not necessarily a unit modulo Nth powers. Rather, there is a natural exact sequence

$$0 \to \mathcal{O}(S)^\times/(\mathcal{O}(S)^\times)^N \to \mathrm{H}^1(S, \mu_N) \to \mathrm{Pic}(S)[N] \to 0.$$

which to $\chi \in \mathrm{H}^1(S, \mathbf{Z}/N)$ and $u \in \mathrm{H}^1(S, \mu_N)$ associates an Azumaya algebra $\mathcal{A}(\chi, u)$ of degree N on S, which is called the cyclic algebra associated to the pair (χ, u). When $S = \operatorname{Spec} k$ is the spectrum of a field, this coincides with the classical cyclic algebra construction by [20, Props. 2.5.2, 4.7.3]. Composing with the natural coboundary Brauer class map $\mathrm{H}^1(S, \mathrm{PGL}_N) \to \mathrm{H}^2(S, \mathbf{G}_m)$, we arrive at the well-known result that the Brauer class of the cyclic algebra $\mathcal{A}(\chi, u)$ in $\mathrm{H}^2(S, \mathbf{G}_m)$ coincides with the image, which we denote by $[\chi, u]$, of the cup product $\chi \cup u$ under the natural map $\mathrm{H}^2(S, \mu_N) \to \mathrm{H}^2(S, \mathbf{G}_m)$.

We now give a stack-theoretic interpretation, building on Lieblich [33, Sec. 4.3]. The cup product pairing on $\mathrm{H}^1(S, \mathbf{Z}/N \times \mu_N) = \mathrm{H}^1(S, \mathbf{Z}/N) \times \mathrm{H}^1(S, \mu_N)$, followed by the natural map $\mathrm{H}^2(S, \mu_N) \to \mathrm{H}^2(S, \mathbf{G}_m)$, gives rise to a functorial assignment $(\chi, u) \mapsto [\chi, u]$ on cohomology $\mathrm{H}^1(S, \mathbf{Z}/N \times \mu_N) \to \mathrm{H}^2(S, \mathbf{G}_m)$, which in turn corresponds to a Brauer class on the classifying stack $\mathrm{B}(\mathbf{Z}/N \times \mu_N)$.

Using the Leray spectral sequence in flat cohomology, one can derive a decomposition

$$\begin{aligned} \mathrm{H}^2(\mathrm{B}(\mathbf{Z}/N \times \mu_N), \mathbf{G}_m) &\cong \mathbf{Z}/N \oplus \mathrm{H}^1(S, \mathrm{Pic}_{\mathrm{B}(\mathbf{Z}/N\times\mu_N)/S}) \oplus \mathrm{H}^2(S, \mathbf{G}_m) \\ &\cong \mathbf{Z}/N \oplus \mathrm{H}^1(S, \mathbf{Z}/N \times \mu_N) \oplus \mathrm{H}^2(S, \mathbf{G}_m). \end{aligned} \tag{1}$$

Here we have utilized isomorphisms $\mathrm{Pic}_{\mathrm{B}(\mathbf{Z}/N\times\mu_N)/S} \cong \mathscr{H}om(\mathbf{Z}/N \times \mu_N, \mathbf{G}_m) \cong \mathbf{Z}/N \times \mu_N$, where the first is canonical and the second follows from Cartier duality.

A computation similar to [33, Sec. 4.3] then shows that the Brauer class $\kappa \in \mathrm{B}(\mathbf{Z}/N \times \mu_N)$, arising from the cup product pairing, is a generator of the $\mathbf{Z}/N$ factor in the decomposition (1).

2.4 The obstruction theory of Clark and O'Neil

Let $\mathcal{L}$ be a relatively ample line bundle of degree N on an elliptic curve $p\colon E \to S$, so that $\mathcal{L}$ defines an S-embedding $E \hookrightarrow \mathbf{P}(p_*\mathcal{L})$, where $p_*\mathcal{L}$ is a rank N vector bundle on S by Riemann–Roch. The S-scheme of S-automorphisms $\mathrm{PGL}_N^{\mathcal{L}}$ of $\mathbf{P}(p_*\mathcal{L})$ is a typically non-split form of PGL_N given specifically by $\mathrm{GL}_N^{\mathcal{L}}/\mathbf{G}_m$, where $\mathrm{GL}_N^{\mathcal{L}}$ is the sheaf of automorphisms of the vector bundle $p_*\mathcal{L}$ over S. If $p_*\mathcal{L}$ is trivial, then these forms will be split. The subgroup of $\mathrm{PGL}_N^{\mathcal{L}}$ coming from translations of the elliptic curve agrees with $E[N]$. Indeed, if $x \in E(T)$ is a section over some S-scheme T, then $x^*\mathcal{L} \cong \mathcal{L}$ if and only $x \in E[N](T)$. It follows that sections of $E[N]$ extend to give automorphisms of $\mathbf{P}(p_*\mathcal{L})$. The induced map $E[N] \hookrightarrow \mathrm{PGL}_N^{\mathcal{L}}$ is a typically twisted form of the standard non-toral cyclic subgroup $\mathbf{Z}/N \times \mu_N \subseteq \mathrm{PGL}_N$ utilized in Section 2.3. Note that it is twisted both in the sense that $E[N]$ is only étale-locally isomorphic (in the non-supersingular case) to $\mathbf{Z}/N \times \mu_N$ and it is also twisted in the sense that even given a full level structure and a trivialization of $p_*\mathcal{L}$, the associated embedding $\mathbf{Z}/N \times \mu_N \hookrightarrow \mathrm{PGL}_N$ is not *a priori* conjugate to the standard non-toral cyclic subgroup over S.

In any case, by pulling back, we obtain a commutative diagram of central extensions

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbf{G}_m & \longrightarrow & \mathcal{G}_{\mathcal{L}} & \longrightarrow & E[N] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbf{G}_m & \longrightarrow & \mathrm{GL}_N^{\mathcal{L}} & \longrightarrow & \mathrm{PGL}_N^{\mathcal{L}} & \longrightarrow & 0, \end{array} \tag{2}$$

where $\mathcal{G}_{\mathcal{L}}$ is a nonabelian affine algebraic group scheme, the theta group of Mumford associated to the pair $(E, \mathcal{L})$; see [44].

Definition 2.8. Associated to the theta group $\mathcal{G}_{\mathcal{L}}$ is the **period-index obstruction map**

$$Ob_{\mathcal{L}}\colon \mathrm{H}^1(S, E[N]) \to \mathrm{H}^2(S, \mathbf{G}_m),$$

which is the boundary map in non-abelian cohomology associated to the short exact sequence in the top row of (2). We will write Ob for the special case when $\mathcal{L} = \mathcal{O}(N0_E)$ is the line bundle associated to the origin of E with multiplicity N.

The period-index obstruction map gets its name from the following result.

Proposition 2.9 ([48], [12]). *Let k be a field. If $X \in \mathrm{H}^1(\operatorname{Spec} k, E)$ has $\operatorname{per}(X) = N$, then $\operatorname{ind}(X) = N$ if and only if for some lift Y of X to $\mathrm{H}^1(\operatorname{Spec} k, E[N])$, the period-index obstruction $Ob(Y)$ vanishes.*

A result of Zarhin shows how the period-index obstruction map and the Weil pairing are related.

Proposition 2.10 ([73]). *The Weil pairing in cohomology can be expressed via the period-index obstruction map $Ob_{\mathcal{L}}$ as*

$$[Y, Z]_N = Ob_{\mathcal{L}}(Y + Z) - Ob_{\mathcal{L}}(Y) - Ob_{\mathcal{L}}(Z)$$

for $Y, Z \in \mathrm{H}^1(S, E[N])$.

Sketch of proof. By definition, the theta group $\mathcal{G}_{\mathcal{L}}$ is a central extension of $E[N]$ by $\mathbf{G}_m$ and as such there is a corresponding alternating pairing $E[N] \times E[N] \to \mathbf{G}_m$ associated to the central extension. Zarhin proves that the induced bilinear pairing $[-,-]_{\mathcal{L}} \colon \mathrm{H}^1(S, E[N]) \times \mathrm{H}^1(S, E[N])$ on cohomology satisfies

$$[Y, Z]_{\mathcal{L}} = Ob_{\mathcal{L}}(Y + Z) - Ob_{\mathcal{L}}(Y) - Ob_{\mathcal{L}}(Z).$$

It is just a statement about the connection between the boundary map in non-abelian cohomology and the pairing associated to the central extension. However, the pairing $[Y, Z]_{\mathcal{L}}$ coincides with the Weil pairing $[Y, Z]_N$ by Mumford [45, (5) on p.228]. □

Recall that a function $f \colon A \to B$ of abelian groups is **quadratic** if $f(nx) = n^2 f(x)$ for all integers n and if the symmetric function $b_f(x, y) = f(x + y) - f(x) - f(y)$ is bilinear. By Proposition 2.10, $b_{Ob_{\mathcal{L}}}$ is bilinear. When $\mathcal{L}$ is a symmetric line bundle on E, meaning that $[-1]^*\mathcal{L} \cong \mathcal{L}$, then $Ob_{\mathcal{L}}$ is additionally quadratic with associated bilinear form $b_{Ob_{\mathcal{L}}} = [-,-]_N$ given by the cohomological Weil pairing by Proposition 2.10. To see this, Mumford uses an isomorphism $[-1]^*\mathcal{L} \cong \mathcal{L}$ to construct, for any integer n, a group endomorphism $\delta_n \colon \mathcal{G}_{\mathcal{L}} \to \mathcal{G}_{\mathcal{L}}$ fitting into a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbf{G}_m & \longrightarrow & \mathcal{G}_{\mathcal{L}} & \longrightarrow & E[N] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle n^2} & & \downarrow{\scriptstyle \delta_n} & & \downarrow{\scriptstyle n} & & \\ 1 & \longrightarrow & \mathbf{G}_m & \longrightarrow & \mathcal{G}_{\mathcal{L}} & \longrightarrow & E[N] & \longrightarrow & 0 \end{array}$$

of exact sequences. This implies immediately the relation $Ob_{\mathcal{L}}(nY) = n^2 Ob_{\mathcal{L}}(Y)$ so that $Ob_{\mathcal{L}}$ is quadratic.

Example 2.11. The line bundle $\mathcal{O}(N0_E)$ is evidently symmetric, so that Ob is a quadratic function with associated bilinear form given by the Weil pairing.

When $\mathcal{L}$ is symmetric and the degree N is odd, it follows that we can compute

$$Ob_{\mathcal{L}}(Y) = \tfrac{1}{2}[Y, Y]_N$$

in $\mathrm{H}^2(S, \mathbf{G}_m)$. Note here that the alternating pairing $E[N] \times E[N] \to \mathbf{G}_m$ becomes symmetric in cohomology $\mathrm{H}^1(S, E[N]) \times \mathrm{H}^1(S, E[N]) \to \mathrm{H}^2(S, \mathbf{G}_m)$.

Now, we specialize to the case where we have a symplectic full level N structure, in a sense that we will make precise. We consider the standard symplectic bilinear form

$$(\mathbf{Z}/N \times \mu_N) \times (\mathbf{Z}/N \times \mu_N) \to \mathbf{G}_m$$

induced from the evaluation pairing, which takes the form $((a,\zeta),(b,\xi)) \mapsto \zeta^b \xi^{-a}$. A full level N structure on an elliptic curve E is an isomorphism of group schemes $\varphi\colon E[N] \to \mathbf{Z}/N \times \mu_N$;[3] we say the full level N structure φ is symplectic if it is an isometry from the Weil pairing on $E[N]$ to the standard symplectic form on $\mathbf{Z}/N \times \mu_N$.

We remark that over a field, the moduli space of elliptic curves with a symplectic full level N structure is geometrically connected, and is a component of the moduli space of elliptic curves with a full level N structure. For more remarks on this type of level structure, see [52, Section 4.1].

Given any full level N structure there is an induced map on cohomology

$$\mathrm{H}^1(\varphi)\colon \mathrm{H}^1(S, E[N]) \to \mathrm{H}^1(S, \mathbf{Z}/N \times \mu_N) = \mathrm{H}^1(S, \mathbf{Z}/N) \times \mathrm{H}^1(S, \mu_N)$$

so that to $Y \in \mathrm{H}^1(S, E[N])$ there is corresponding tuple $(\chi, u) \in \mathrm{H}^1(S, \mathbf{Z}/N) \times \mathrm{H}^1(S, \mu_N)$. We now proceed to show how this is related to the Brauer class $[\chi, u] \in \mathrm{H}^2(S, \mathbf{G}_m)$ of the cyclic algebra $\mathcal{A}(\chi, u)$. First, we need the following.

Lemma 2.12. *The standard symplectic form on $\mathbf{Z}/N \times \mu_N$ induces a pairing on cohomology*

$$[-,-]_\kappa\colon \mathrm{H}^1(S, \mathbf{Z}/N \times \mu_N) \times \mathrm{H}^1(S, \mathbf{Z}/N \times \mu_N) \to \mathrm{H}^2(S, \mathbf{G}_m)$$

given by

$$\begin{aligned}[(\chi_0, u_0), (\chi_1, u_1)]_\kappa &= [\chi_0 + \chi_1, u_0 u_1] - [\chi_0, u_0] - [\chi_1, u_1] \\ &= [\chi_0, u_1] + [\chi_1, u_0].\end{aligned}$$

Proof. After Zarhin [73], the important thing to check is that pulling back the central extension $1 \to \mathbf{G}_m \to \mathrm{GL}_N \to \mathrm{PGL}_N \to 1$ along the homomorphism $\mathbf{Z}/N \times \mu_N \hookrightarrow \mathrm{PGL}_N$ yields a central extension $1 \to \mathbf{G}_m \to \mathcal{H}_N \to \mathbf{Z}/N \times \mu_N \to 1$, whose associated 2-cocycle determines the standard symplectic form. This verification is routine: one lifts elements of $\mathbf{Z}/N \times \mu_N$ to elements of GL_N (which we have already done in the previous section) and then one computes the commutator.[4] For example, the commutator between the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

and the diagonal matrix $(1, \zeta, \ldots, \zeta^{N-1})$ is the constant diagonal matrix ζ in the center. □

Now, we give our version of the obstruction theory of O'Neil and Clark.

Proposition 2.13. *Let $\mathcal{L}$ be a symmetric line bundle of degree N on E and suppose that $\varphi\colon E[N] \to \mathbf{Z}/N \times \mu_N$ is a symplectic full level N structure and that $Y \in \mathrm{H}^1(S, E[N])$ corresponds to the tuple $\mathrm{H}^1(\varphi)(Y) = (\chi, u) \in \mathrm{H}^1(S, \mathbf{Z}/N) \times \mathrm{H}^1(S, \mu_N)$. If N is odd, then*

$$Ob_{\mathcal{L}}(Y) = \tfrac{1}{2}[Y, Y]_N = [\chi, u]$$

in $\mathrm{H}^2(S, \mathbf{G}_m)$. If N is even, then

$$Ob_{\mathcal{L}}(Y) = [\chi, u] + [\chi, v] + [\sigma, u]$$

for classes $v \in \mathrm{H}^1(S, \mu_2)$ and $\sigma \in \mathrm{H}^1(S, \mathbf{Z}/2)$ that depend only on E, N, φ, and $\mathcal{L}$.

[3] Often, it is φ^{-1} which is called the full level N structure; moreover, when N is not invertible, it is usually more desirable to use Drinfeld level N structures to capture supersingular phenomena; see [26].

[4] The group $\mathcal{H}_N$ appearing here is a Heisenberg group.

Proof. The functorial assignment $Ob_{\mathcal{L}}\colon \mathrm{H}^1(S, E[N]) \to \mathrm{H}^2(S, \mathbf{G}_m)$ corresponds by Yoneda to a Brauer class on the classifying stack $\mathrm{B}(E[N])$. A full level N structure $\varphi\colon E[N] \to \mathbf{Z}/N \times \mu_N$ induces an equivalence of stacks $\mathrm{B}(\varphi)\colon \mathrm{B}(E[N]) \to \mathrm{B}(\mathbf{Z}/N \times \mu_N)$. Applying $\mathrm{B}(\varphi)^{-1*}$ to the Brauer class on $\mathrm{B}(E[N])$ corresponding to $Ob_{\mathcal{L}}$, we obtain a class $\mathrm{B}(\varphi)^{-1*}(Ob_{\mathcal{L}})$ in $\mathrm{H}^2(\mathrm{B}(\mathbf{Z}/N \times \mu_N), \mathbf{G}_m)$, and we wish to view this class with respect to the decomposition (1).

Given a Brauer class on $\mathrm{B}(\mathbf{Z}/N \times \mu_N)$ determined via (1) by an integer $n \pmod N$ and classes $v \in \mathrm{H}^1(S, \mu_N)$, $\sigma \in \mathrm{H}^1(S, \mathbf{Z}/N)$, and $\alpha \in \mathrm{H}^2(S, \mathbf{G}_m)$, the associated functorial assignment $\mathrm{H}^1(S, \mathbf{Z}/N \times \mu_N) \to \mathrm{H}^2(S, \mathbf{G}_m)$ is

$$(\chi, u) \mapsto n[\chi, u] + [\chi, v] + [\sigma, u] + p^*\alpha \tag{3}$$

where $p\colon \mathrm{B}(\mathbf{Z}/N \times \mu_N) \to S$ is the structure morphism and where we consider the cup products via the natural map $\mathrm{H}^2(S, \mu_N) \to \mathrm{H}^2(S, \mathbf{G}_m)$.

We now consider the representation of $\mathrm{B}(\varphi)^{-1*}(Ob_{\mathcal{L}})$ with respect to (3). Since $Ob_{\mathcal{L}}(0) = 0$, we see that $\alpha = 0$. Since φ is symplectic, the cohomological pairing induced by $\mathrm{B}(\varphi)^{-1*}(Ob_{\mathcal{L}})$, which is

$$n[\chi_0, u_1] + n[\chi_1, u_0]$$

by Proposition 2.10 and (3) (since the linear part does not contribute), must agree with that induced by the standard symplectic pairing on $\mathbf{Z}/N \times \mu_N$, which is

$$((\chi_0, u_0), (\chi_1, u_1)) = [\chi_0 + \chi_1, u_0 + u_1] - [\chi_0, u_0] - [\chi_1, u_1] = [\chi_0, u_1] + [\chi_1, u_0]$$

by Lemma 2.12. From this, we see that $n \equiv 1 \pmod N$. Since $Ob_{\mathcal{L}}$ is quadratic because $\mathcal{L}$ is symmetric, we see that if N is odd, then $v = \sigma = 0$. If N is even, then we see that $[2\chi, u^2]+[2\chi, v]+[\sigma, u^2] = 4([\chi, u]+[\chi, v]+[\sigma, u])$, which after cancellation gives $2([\chi, v] + [\sigma, u]) = 0$. Since this is true no matter the choice of χ and u, and even remains true after arbitrary field extensions, we see that v and σ must be 2-torsion, which completes the proof. □

The proof of the following refinement of Proposition 2.13 is given in [49].

Proposition 2.14. *Let E be an elliptic curve with a symplectic full level N structure $\varphi\colon E[N] \to \mathbf{Z}/N \times \mu_N$ and let $P = \varphi^{-1}(1, 1)$. If $\mathcal{L} = \mathcal{O}(0_E + P + \cdots + (N-1)P)$ then the corresponding class $v \in \mathrm{H}^1(S, \mu_N)$ in Proposition 2.13 vanishes. In particular, in the notation of that proposition,*

$$Ob_{\mathcal{L}}(Y) = [\chi + \sigma, u]$$

for some $\sigma \in \mathrm{H}^1(S, \mathbf{Z}/N)$ that is trivial whenever N is odd.

Proof. Arguing as in Section 2.3 or [33, Sec. 4.3], we see that $\mathrm{H}^2(\mathrm{B}(\mathbf{Z}/N), \mathbf{G}_m) \cong \mathrm{H}^1(S, \mu_N) \oplus \mathrm{H}^2(S, \mathbf{G}_m)$. This is compatible with the computation of the cohomology of $\mathrm{B}(\mathbf{Z}/N \times \mu_N)$ of (1), which means that we can find v by pullback of $\mathrm{B}(\varphi)^{-1}(Ob_{\mathcal{L}})$ from $\mathrm{B}(\mathbf{Z}/N \times \mu_N)$ to $\mathrm{B}(\mathbf{Z}/N)$. The Brauer class corresponding to v on $\mathrm{B}(\mathbf{Z}/N)$ is that of the projective representation $\rho\colon \mathbf{Z}/N \to \mathrm{PGL}_N^{\mathcal{L}}$ induced by $\mathbf{Z}/N \times 1 \xrightarrow{\varphi^{-1}} E[N] \hookrightarrow \mathrm{PGL}_N^{\mathcal{L}}$.

In general, computing the Brauer class on $\mathrm{B}(\mathbf{Z}/N)$ from the projective representation is possible as follows. Let $t_P\colon E \to E$ denote translation by P and choose an isomorphism $t_P^*\mathcal{L} \cong \mathcal{L}$. Pulling back by t_P gives an invertible map $\tau_P\colon p_{\mathcal{L}} \to p_* t_P^* \mathcal{L} \cong p_* \mathcal{L}$ that lifts $\rho(P)$ to $\mathrm{GL}_N^{\mathcal{L}}$ via $\mathrm{GL}_N^{\mathcal{L}} \to \mathrm{PGL}_N^{\mathcal{L}}$. As $\rho(P)$ has order N in $\mathrm{PGL}_N^{\mathcal{L}}$, the Nth power of τ_P is a unit multiple of the identity $b \cdot I_N$ since the center of $\mathrm{GL}_N^{\mathcal{L}}$ is still $\mathbf{G}_m$. The class of b in $\mathrm{H}^1(S, \mu_N)$ is then the Brauer class on $\mathrm{B}(\mathbf{Z}/N)$ corresponding to ρ. To see this, note that ρ lifts to a representation $\mathbf{Z}/N \to \mathrm{GL}_N^{\mathcal{L}}$ if and only if we can rescale τ_P by a unit to obtain τ_P' such that $(\tau_P')^N = I_N$. If $b = c^N$, then $\tau_P' = c^{-1}\tau_P$ works, and conversely.

We have to show that in the setup of the proposition, this b is itself an Nth power, cf. [47, Corollary 2.8]. The line bundle $\mathcal{L}$ is the divisor class of the divisor $0_E + P + \cdots + (N-1)P$. This divisor is in fact invariant

by translation by P so there is a preferred identification of $\mathcal{L}$ and $t_P^*\mathcal{L}$. Specifically, $\mathcal{L} \simeq \mathcal{O}(0_E) \otimes \mathcal{O}(P) \otimes \cdots \otimes \mathcal{O}((N-1)P)$ and $t_P^*\mathcal{L}$ is a cyclic permutation. In particular, we can arrange for τ_P to act on

$$p_*\mathcal{L} \cong p_*\mathcal{O}(0_E) \oplus p_*\mathcal{O}(P) \oplus \cdots \oplus p_*\mathcal{O}((N-1)P)$$

via a cyclic permutation (we use here that the genus of E is 1 over S), which has associated unit element $b = 1$. This completes the proof. □

When E has full rational N-torsion over a field k (necessarily containing a primitive Nth root of unity), O'Neil [48, Prop. 3.4] states the first part of Proposition 2.13, but for any N, and then provides a correction in [49] which amounts to Proposition 2.14. Around the same time, again assuming that E has full rational N-torsion, Clark [12, Sec. 3.2] states the second part of the result, but for all N, while pointing out the issue with $N = 2$ that was uncovered by a referee, which implies that in general v and σ are non-zero for the obstruction map Ob corresponding to $\mathcal{O}(N0_E)$. Our version of the result, while holding over a general base S, utilizes our more general notion of full level N structure, which in particular does not presuppose the presence of Nth roots of unity.

Remark 2.15. Using oriented automorphisms of $p_*\mathcal{L}$, one can obtain an oriented theta group, which is an extension of $E[N]$ by μ_N. Then, the definition of the Weil pairing, the period-obstruction map, and the above lemma carry over with values in $\mathrm{H}^2(S, \mu_N)$ as well. Specifically, we can pull back the extension

$$1 \to \mu_N \to \mathrm{SL}_N^{\mathcal{L}} \to \mathrm{PGL}_N^{\mathcal{L}} \to 1$$

along $E[N] \to \mathrm{PGL}_N^{\mathcal{L}}$. Propositions 2.10, 2.13, and 2.14 now hold with target in $\mathrm{H}^2(S, \mu_N)$ instead of $\mathrm{H}^2(S, \mathbf{G}_m)$ with the exception that in the proofs of Propositions 2.13 and 2.14, in order to conclude that the contribution of the constant class classes $\mathrm{H}^2(S, \mu_N)$ to $Ob_{\mathcal{L}}$ vanishes, we need to know that $c_1(p_*\mathcal{L}) = 0$, which is always true locally on S. The details are left to the reader.

Warning 2.16. We will use Proposition 2.14 in the proof of Theorem C, but note that we cannot improve the statement to split μ_N-gerbes, despite the previous remark. This is because a later result, Lemma 3.20, does not apply to μ_N-cohomology classes, as Example 3.8 shows.

3 Proofs

3.1 Splitting μ_N-gerbes

As explained in the introduction, we are interested in the following general question, which motivates our approach to the problem of splitting Brauer classes by genus 1 curves.

We first recall that, for any proper geometrically connected scheme X over a field k, a consequence of the long exact sequence of cohomology associated to the Kummer sequence are the exact sequences:

$$0 \to k^\times/(k^\times)^N \to \mathrm{H}^1(X, \mu_N) \to \mathrm{Pic}(X)[N] \to 0,$$

$$0 \to \mathrm{Pic}(X)/N\,\mathrm{Pic}(X) \to \mathrm{H}^2(X, \mu_N) \to \mathrm{H}^2(X, \mathbf{G}_m)[N] \to 0.$$

When X is projective, the right-most term in the second statement is $\mathrm{Br}(X)[N]$ via Gabber's $\mathrm{Br} = \mathrm{Br}'$ result; see [15]. In particular, we can view classes in $\mathrm{H}^2(X, \mu_N)$ as lifts of N-torsion Brauer classes.

Question 3.1. Let k be a field and $\beta \in \mathrm{H}^2(\mathrm{Spec}\, k, \mu_N)$. Is there a smooth proper geometrically connected k-scheme X such that β pulls back to zero in $\mathrm{H}^2(X, \mu_N)$?

A class $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$ can be considered as the cohomology class associated to a μ_N-gerbe, hence if it pulls back to zero in $\mathrm{H}^2(X, \mu_N)$ then we say that X splits the μ_N-gerbe β. If we drop the hypothesis that X is geometrically connected, we can of course just take X to be the spectrum of a finite field extension that splits β. One might be tempted to take X to be a Severi–Brauer variety associated to β, but Lemma 3.2 below shows that these varieties do not split μ_N-gerbes.

To think about this question, consider the Leray–Serre spectral sequence

$$\mathrm{E}_2^{s,t} = \mathrm{H}^s(\operatorname{Spec} k, \mathrm{R}p^t_*\mu_n) \Longrightarrow \mathrm{H}^{s+t}(X, \mu_n)$$

for the sheaf μ_N associated to the structure morphism $p\colon X \to \operatorname{Spec} k$. We have $\mathrm{R}p^0_*\mu_n \cong \mu_n$ since X is geometrically connected and $\mathrm{R}p^1_*\mu_n \cong \operatorname{Pic}_{X/k}[n]$ since X is proper over k. Hence the exact sequence of low-degree terms, together with the exact sequence in degree 1 recalled above, reads as

$$0 \to \operatorname{Pic}(X)[N] \to \operatorname{Pic}_{X/k}[N](k) \xrightarrow{\mathrm{d}_2^{0,1}} \mathrm{H}^2(\operatorname{Spec} k, \mu_N) \to \mathrm{H}^2(X, \mu_N) \tag{4}$$

where $\mathrm{d}_2^{0,1}$ is the appropriate differential and the final map is the pull back in cohomology. This exact sequence shows that X splits the μ_N-gerbe β if and only if β arises as the differential of an N-torsion point on the Picard scheme $\operatorname{Pic}_{X/k}$. In particular, we have the following.

Lemma 3.2. *Let X be smooth proper geometrically connected k-scheme. The pullback map $\mathrm{H}^2(\operatorname{Spec} k, \mu_n) \to \mathrm{H}^2(X, \mu_n)$ is injective, in other words, X does not split any nontrivial μ_N-gerbe over k, if and only if the differential $d_2^{0,1}\colon \operatorname{Pic}_{X/k}[N](k) \to \mathrm{H}^2(k, \mu_N)$ vanishes.*

As a special case, the lemma shows that if $\operatorname{Pic}_{X/k}[N](k) = 0$, then $\mathrm{H}^2(\operatorname{Spec} k, \mu_N) \to \mathrm{H}^2(X, \mu_N)$ is injective and hence X does not split any μ_N-gerbe. This condition holds, in particular, whenever the Picard group of X is geometrically torsion-free, e.g., for K3 surfaces, Severi–Brauer varieties, and for smooth complete intersections of dimension at least 2.

Another special case is that of Enriques surfaces X: if X is classical (e.g., if the characteristic of k is not 2), then $\operatorname{Pic}(X)[2] \cong \operatorname{Pic}_{X/k}[2](k) \cong \mathbf{Z}/2$ is generated by the canonical line bundle; if X is singular or supersingular in characteristic 2, then $\operatorname{Pic}_{X/k}[2] \cong \mu_2$ or α_2, respectively, so the group of k-rational points is 0 (see [7]). In either case, $\mathrm{d}_2^{0,1} = 0$ so Enriques surfaces cannot split μ_2-gerbes.

We will now give some examples where genus 1 curves do split μ_N-gerbes and others where they split Brauer classes but not their associated μ_N-gerbes. More subtly, we will give examples where a genus 1 curve X does not split any μ_N-gerbe lifting α of period N, but that X does split some μ_{NM}-gerbe lifting α for $M > 1$. Many of these examples rely on the following, cf. [11, Theorem 2.1].

Lemma 3.3. *Let X be a genus 1 curve over a field k with Jacobian $\operatorname{Pic}^0_{X/k}$. There is a commutative diagram*

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \operatorname{Pic}^0(X) & \longrightarrow & \operatorname{Pic}^0_{X/k}(k) & \longrightarrow & \operatorname{Br}(k) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \operatorname{Pic}(X) & \longrightarrow & \operatorname{Pic}_{X/k}(k) & \longrightarrow & \operatorname{Br}(k) \\
 & & \downarrow & & \downarrow & & \\
 & & \mathbf{Z}\cdot\operatorname{ind}(X) & \longrightarrow & \mathbf{Z}\cdot\operatorname{per}(X). & & \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

In particular, letting $\mathrm{Br}^0(X/k) = \mathrm{im}(\mathrm{Pic}^0_{X/k}(k) \to \mathrm{Br}(k))$ *and* $\mathrm{Br}(X/k) = \mathrm{im}(\mathrm{Pic}_{X/k}(k) \to \mathrm{Br}(k)) = \ker(\mathrm{Br}(k) \to \mathrm{Br}(X))$*, there is an exact sequence*

$$0 \to \mathrm{Br}^0(X/k) \to \mathrm{Br}(X/k) \to \mathbf{Z}/(\mathrm{ind}(X)/\mathrm{per}(X)) \to 0. \tag{5}$$

Corollary 3.4. *Let E be an elliptic curve over a field k such that $E(k)$ is an N-torsion group. Let X be an E-torsor such that $\mathrm{per}(X) = \mathrm{ind}(X)$. If X splits a Brauer class $\alpha \in \mathrm{Br}(k)[N]$, then it splits the unique lift $\beta \in \mathrm{H}^2(\mathrm{Spec}\, k, \mu_N)$ of α.*

Proof. Indeed, by Lemma 3.3 we see that $\alpha \in \mathrm{Br}^0(X/k)$, hence $\alpha = \mathrm{d}_2^{0,1}(P)$ for some point $P \in E(k) = \mathrm{Pic}^0_{X/k}(k)$. However, since $E(k)$ is an N-torsion group, $P \in \mathrm{Pic}_{X/k}[N](k)$. Compatibility of the Leray–Serre spectral sequences for μ_N and $\mathbf{G}_m$-cohomology provides a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}_{X/k}[N](k) & \xrightarrow{\mathrm{d}_2^{0,1}} & \mathrm{H}^2(\mathrm{Spec}\, k, \mu_N) \\ \downarrow & & \\ \mathrm{Pic}^0_{X/k}(k) & & \downarrow \\ \downarrow & & \\ \mathrm{Pic}_{X/k}(k) & \xrightarrow{\mathrm{d}_2^{0,1}} & \mathrm{H}^2(\mathrm{Spec}\, k, \mathbf{G}_m) \end{array}$$

showing that β, considered as an element of $\mathrm{H}^2(\mathrm{Spec}\, k, \mu_N)$, is in the image of a class from $\mathrm{Pic}_{X/k}[N](k)$, so that X splits the μ_N-gerbe β. □

Example 3.5. If k has characteristic not 2, then the quaternion algebra $[a, b]$ is split by the genus 1 curve X defined by

$$y^2 = ax^4 + b.$$

Geometrically, one can see this since $(x, y) \mapsto (x^2, y)$ determines a (finite degree 2) morphism from X to the conic $y^2 = ax^2 + b$ determined by $[a, b]$. The relative Brauer group $\mathrm{Br}(X/k)$ was studied by [21] and [11, Sec. 5.2.1] in terms of the Jacobian E of X, which is defined by $y^2 = x^3 - 4abx$, giving examples of the phenomenon in Corollary 3.4. Here, when $[a, b]$ is nonsplit, one has $\mathrm{per}(X) = \mathrm{ind}(X) = 2$ and in general one can find examples where $E(k)$ is 2-torsion. For example, this is the case for $a = 2$ and $b = 3$ where the Jacobian is given up to isomorphism by $y^2 = x^3 - 24x$, the curve `2304.n1` from `lmfdb.org` [34], which has $E(\mathbf{Q}) \cong \mathbf{Z}/2$. Thus, the μ_2-gerbe $2 \cup 3 \in \mathrm{H}^2(\mathrm{Spec}\, \mathbf{Q}, \mu_2)$ is split by the genus 1 curve that is the unique smooth proper model of $y^2 = 2x^4 + 3$.

Example 3.6. An analysis similar to the proof of Corollary 3.4 shows that if X is an E-torsor with $E(k)$ a torsion group, and the relative Brauer group $\mathrm{Br}(X/k)$ is not cyclic, then there must be classes of $\mathrm{H}^2(\mathrm{Spec}\, k, \mu_N)$ for some N split by X. An explicit example is given in [11, Sec 5.2.3].

Example 3.7. We can also examine the proof of Corollary 3.4 to find more subtle phenomena. If E is an elliptic curve with $E(k) \cong \mathbf{Z}/NM$ generated by a point P, where $N, M > 1$, and X is and E-torsor with $\mathrm{d}_2^{0,1}(P) = \alpha \in \mathrm{Br}(k)$ having period N, then we see that X does not split the μ_N-gerbe associated to α though it does split the associated μ_{NM}-gerbe, hence also α. An explicit example can be taken from our proof of Theorem A in Section 3.4. Let E be the elliptic curve

$$y^2 + xy + 4y = x^3 + 4x^2,$$

which is `130.b4` from `lmfdb.org` [34] and satisfies $E(\mathbf{Q}) \cong \mathbf{Z}/4$. For any $\chi \in \mathrm{H}^1(\mathrm{Spec}\, \mathbf{Q}, \mathbf{Z}/4)$ we define an E-torsor X_χ in Section 3.2 such that $\mathrm{d}_2^{0,1}(P) = \chi \cup 2^6 = 2(\chi \cup 2)$, where $\chi \cup 2$ is the quartic cyclic symbol.

Hence the image of $\mathrm{d}_2^{0,1} : E[4](\mathbf{Q}) \to \mathrm{H}^2(\operatorname{Spec}\mathbf{Q}, \mu_4)$ is at most a subgroup of order 2, which is nontrivial if and only if the cyclic algebra $[\chi, 2]$ has period 4. In this case, X_χ splits the μ_4-gerbe associated to the Brauer class $\alpha = 2[\chi, 2]$, but not the associated μ_2-gerbe.

Example 3.8. Let k be a global field and let N be invertible in k. Fix a positive integer M dividing N. Sharif showed in [56] that for any elliptic curve E over k, there exists an E-torsor X with $\operatorname{per}(X) = N$ and $\operatorname{ind}(X) = MN$. (Clark and Sharif [14] had previously shown this result when $M = N$.) If $M > 1$, then it follows from the exact sequence (5) that X splits some non-zero Brauer classes, specifically the period-index obstruction classes $Ob(Y)$ where Y ranges over the lifts of X to $\mathrm{H}^1(\operatorname{Spec} k, E[N])$. If E is chosen so that $E[N](k) = 0$, then we see that X cannot split any μ_N-gerbe. This gives examples of the phenomenon of a genus 1 curve splitting a Brauer class α but not any associated μ_N-gerbe β. In particular, over $\mathbf{Q}$, if $N \geqslant 11$ is a prime, then $E[N](\mathbf{Q}) = 0$ for any elliptic curve by Mazur's theorem [37] and there is some Brauer class α of order N split by an E-torsor. In fact, there are infinitely many such by [14, Thm. 2]. This establishes the existence of Brauer classes α split by a genus 1 curve where the associated μ_N-gerbe is not split by any genus 1 curve.

Finally, we examine the case of splitting μ_N-gerbes over local fields. Here is the non-archimedean case.

Proposition 3.9. *If K is a non-archimedean local field and $N \geqslant 2$, then every μ_N-gerbe $\beta \in \mathrm{H}^2(\operatorname{Spec} K, \mu_N) \cong \mathbf{Z}/N$ is split by a genus 1 curve.*

Proof. It suffices to consider the case when β has exact order N in $\mathrm{H}^2(\operatorname{Spec} K, \mu_N)$. Indeed, every exact order N element of $\mathrm{H}^2(\operatorname{Spec} K, \mu_{MN})$ is in the image of the natural map $\mathrm{H}^2(\operatorname{Spec} K, \mu_N) \to \mathrm{H}^2(\operatorname{Spec} K, \mu_{MN})$ induced by $\mu_N \hookrightarrow \mu_{MN}$. So, assume that β has exact order N in $\mathrm{H}^2(\operatorname{Spec} K, \mu_N)$. There is an elliptic curve E over K with an exact order N point P. Indeed, as explained to us by Pete Clark, this follows from the existence of Tate curves; see [67]. Let E be the Tate elliptic curve with $E(K) \cong K^\times/(\varpi^N)^{\mathbf{Z}}$, where ϖ is a uniformizer of K. As an element of $K^\times$, ϖ reduces to give an exact order N point of $E(K)$. Let α be the image of β in $\operatorname{Br}(K)$. By the non-degeneracy of the Tate pairing, there is an E-torsor X such that $[P, X]_T = \alpha$. It follows that X splits α. Specifically, viewing P as a K-point of the Jacobian $\operatorname{Pic}_{X/K}$, we see that $\mathrm{d}_2^{0,1}(P) = \alpha$ where the d_2-differential comes from the Leray–Sere spectral sequence for $\mathbf{G}_m$-cohomology. Since P is N-torsion, we also have $\mathrm{d}_2^{0,1}(P) = \beta$, where we view P as a section of $\operatorname{Pic}_{X/K}[N]$ and work in the Leray–Serre spectral sequence for μ_N-cohomology. In particular, X splits the μ_N-gerbe β. □

Now, we consider the real case. To begin, we recall a well-known result about Legendre curves and a classification of the 2-torsion of real elliptic curves.

Lemma 3.10. *An elliptic curve E over a field k of characteristic not 2 has full rational 2-torsion if and only if E is a quadratic twist of a Legendre curve.*

Proof. Given a Weierstrass equation $y^2 = f(x)$ of E, the rational 2-torsion points correspond to roots of $f(x)$. Hence E has full rational 2-torsion if and only if it admits a Weierstrass equation of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$ for some distinct $e_1, e_2, e_3 \in k$. In this case, the change of variables $(x, y) \mapsto \big((e_2 - e_1)x + e_1, (e_2 - e_1)^2 y\big)$ transforms the Weierstrass equation into $(e_2 - e_1)y^2 = x(x - 1)(x - \frac{e_3 - e_1}{e_2 - e_1})$, which is the quadratic twist of a Legendre curve. Conversely, any Legendre curve has full rational 2-torsion, hence any quadratic twist does as well, since negation acts trivially on the group scheme $E[2]$. □

Remark 3.11. The proof of Lemma 3.10 shows that if E has full rational 2-torsion, then it is isomorphic to a Legendre curve if and only if any of the elements $e_j - e_i \in k^\times$ for $i \neq j$ is a square. In particular, over the field of real numbers, every elliptic curve with full rational 2-torsion is isomorphic to a Legendre curve.

Lemma 3.12. *Let E be an elliptic curve over $\mathbf{R}$ with j-invariant $j(E)$.*

(1) *If E has full rational 2 torsion then $j(E) \geqslant 1728$. In this case, there is a unique nontrivial E-torsor X, which has index 2.*

(2) *If E does not have full rational 2 torsion, then $j(E) \leqslant 1728$. In this case, $E[2]$ is isomorphic to the Weil restriction group scheme $R_{\mathbf{C}/\mathbf{R}}\mathbf{Z}/2$ and all E-torsors are split.*

(3) *If $j(E) = 1728$ then E can have full rational 2 torsion or not, depending on the sign in the Weierstrass equation $y^2 = x^3 \mp x$ of E.*

Proof. The 2-torsion group scheme $E[2]$ is an extension $0 \to \mathbf{Z}/2 \to E[2] \to \mathbf{Z}/2 \to 0$. Indeed, every elliptic curve over $\mathbf{R}$ admits a point of order 2 since any cubic polynomial over $\mathbf{R}$ has a root. Since the extension is geometrically split, either $E[2] \cong \mathbf{Z}/2 \times \mathbf{Z}/2$ when E has full rational 2-torsion or $E[2] \cong E_{\mathbf{C}/\mathbf{R}}\mathbf{Z}/2$ when $E[2]$ does not have full rational 2-torsion. Now consider the exact sequence

$$0 \to E(\mathbf{R})/2E(\mathbf{R}) \to \mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E[2]) \to \mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E)[2] \to 0$$

in cohomology.

If E has full rational 2-torsion, then $E(\mathbf{R})$ has two connected components. Since the identity component is 2-divisible, $E(\mathbf{R})/2E(\mathbf{R}) \cong \mathbf{Z}/2$ is isomorphic to the component group of $E(\mathbf{R})$. Since

$$\mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E[2]) \cong \mathrm{H}^1(\operatorname{Spec}\mathbf{R}, \mathbf{Z}/2 \times \mathbf{Z}/2) \cong \mathbf{Z}/2 \times \mathbf{Z}/2,$$

the above exact sequence implies that $\mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E)[2] \cong \mathbf{Z}/2$. However, since any E-torsor has index, and hence period, dividing 2, we deduce that $\mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E) \cong \mathbf{Z}/2$. Thus there is a unique nontrivial E-torsor, which has index 2.

If E does not have full rational 2-torsion, then

$$\mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E[2]) = \mathrm{H}^1(\operatorname{Spec}\mathbf{R}, R_{\mathbf{C}/\mathbf{R}}\mathbf{Z}/2) = \mathrm{H}^1(\operatorname{Spec}\mathbf{C}, \mathbf{Z}/2) = 0,$$

which then implies that $\mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E)[2] = 0$. Again, since every E-torsor has index, hence period, dividing 2, we have that $\mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E) = 0$. Hence all E-torsors are split.

We proceed to prove the statements about the j-invariant. By Lemma 3.10, E has full rational 2-torsion if and only if E is a quadratic twist of a Legendre curve $y^2 = x(x-1)(x-\lambda)$ for some $\lambda \neq 0, 1$. Since twisting preserves the j-invariant, if E has full rational 2-torsion then $j(E) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$. One can compute that $j(E) \geqslant 1728$ and that the minimum value of 1728 is obtained, for example when $\lambda = 1$. Conversely, by continuity, every number $j > 1728$ is obtained as the j-invariant of a Legendre curve, thus every elliptic curve with j-invariant $j(E) > 1728$ is a quadratic twist of a Legendre curve, hence has full rational 2-torsion.

Finally, we remark that the unique elliptic curve E over $\mathbf{R}$ with $j(E) = 1728$ and full rational 2-torsion has Weierstrass equation $y^2 = x^3 - x$, which is `32.a3` in the `lmfdb.org` [34]. The only other elliptic curve E over $\mathbf{R}$ with $j(E) = 1728$, `64.a4` in the `lmfdb.org` [34] with Weierstrass equation $y^2 = x^3 + x$, does not have full rational 2-torsion. These two elliptic curves are quartic twists of each other, cf. [59, Corollary X.5.4.1]. □

Finally, we classify when a genus 1 curves can split the (unique) μ_2-gerbe over $\mathbf{R}$.

Proposition 3.13. *Let $\beta \in \mathrm{H}^2(\operatorname{Spec}\mathbf{R}, \mu_2) \cong \mathbf{Z}/2$ be the μ_2-gerbe corresponding to the unique nontrivial element of $\mathrm{Br}(\mathbf{R})$. Let E be an elliptic curve over $\mathbf{R}$ with j-invariant $j(E)$. Then β is split by an E-torsor if and only if E has full rational 2-torsion, or equivalently if and only if $j(E) > 1728$ or E is the unique elliptic curve with $j(E) = 1728$ and full rational 2-torsion.*

Proof. By Lemma 3.12, we must show that if E has full rational 2-torsion, then the unique nontrivial E-torsor X splits β. Choosing a (necessarily symplectic) full level 2 structure on E, we get an obstruction map of the form

$$Ob(Y) = [\chi, u] + [\chi, v] + [u, \sigma]$$

for $Y \in \mathrm{H}^1(\operatorname{Spec}\mathbf{R}, E[2])$, where χ, u, v, σ are as in Proposition 2.10. Whatever the nature of v, σ, some choice of χ, u (corresponding to some choice of $E[2]$-torsor Y lifting X) will satisfy $Ob(Y) = \alpha$, where α is the Brauer class of β (corresponding to Hamilton's quaternions). By Lemma 3.20, X splits α. Since $\operatorname{per}(X) = \operatorname{ind}(X) = 2$, the exact sequence (5) implies that the exact sequence of low degree terms of the Leray spectral sequence for $\mathbf{G}_m$ on X reads as

$$0 \to \operatorname{Pic}(X) \to E(\mathbf{R}) \to \mathrm{H}^2(\operatorname{Spec}\mathbf{R}, \mathbf{G}_m) \to 0.$$

This implies that $\operatorname{Pic}(X)$ is isomorphic to the connected component of the identity of $E(\mathbf{R})$. In particular, we have $\operatorname{Pic}(X)[2] \cong \mathbf{Z}/2$. Since $E(\mathbf{R})[2]) \cong \mathbf{Z}/2 \times \mathbf{Z}/2$, the exact sequence (4) shows that there must be a non-trivial differential $\operatorname{Pic}_{X/\mathbf{R}}[2](\mathbf{R}) \to \mathrm{H}^2(\operatorname{Spec}\mathbf{R}, \mu_2)$. In other words, X splits β, as desired. □

3.2 Descent via μ_N-isogenies

In this section, we describe the specific tools we will use to prove Theorems A and B. Let

$$0 \to \mu_N \to E \xrightarrow{\varphi} E' \to 0$$

be a μ_N-isogeny with dual isogeny

$$0 \to \mathbf{Z}/N \to E' \xrightarrow{\widehat{\varphi}} E \to 0.$$

Implicitly, in identifying $\ker(\widehat{\varphi}) \cong \mathbf{Z}/N$ we have made a choice of an S-point P of E' of order N. We have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_N & \longrightarrow & E[N] & \longrightarrow & \mathbf{Z}/N & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mu_N & \longrightarrow & E & \longrightarrow & E' & \longrightarrow & 0 \end{array} \tag{6}$$

with exact rows. Taking boundaries we obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{H}^1(S, \mathbf{Z}/N) & \xrightarrow{\delta} & \mathrm{H}^2(S, \mu_N) \\ \downarrow & & \| \\ \mathrm{H}^1(S, E') & \xrightarrow{\delta} & \mathrm{H}^2(S, \mu_N). \end{array}$$

The crux of our argument is the following simple lemma.

Lemma 3.14. *Let $\chi \in \mathrm{H}^1(S, \mathbf{Z}/N)$ have associated E'-torsor X_χ. Then, X_χ splits $\delta(\chi)$.*

Proof. Indeed, X_χ splits the class X_χ itself and hence it splits $\delta(\chi) = \delta(X_\chi)$. □

It remains to compute the boundary map $\delta\colon \mathrm{H}^1(S, \mathbf{Z}/N) \to \mathrm{H}^2(S, \mu_N)$. We can write the cohomological Weil pairing associated to the isogeny φ as a pairing

$$(-,-)_\varphi\colon \mathrm{H}^1(S, \mu_N) \times \mathrm{H}^1(S, \mathbf{Z}/N) \to \mathrm{H}^2(S, \mu_N)$$

as in Definition 2.6. The obstruction to lifting P to an S-point of $E[N]$, via the coboundary map $\delta\colon \mathrm{H}^0(S, \mathbf{Z}/N) \to \mathrm{H}^1(S, \mu_N)$ from the exact sequence (6), gives a distinguished element $\delta(P) \in \mathrm{H}^1(S, \mu_N)$.

Lemma 3.15. *We have $\delta(\chi) = \delta(P) \cup \chi = (\delta(P), \chi)_\varphi$ in $\mathrm{H}^2(S, \mu_N)$.*

This is a special case of the following, more general lemma.

Lemma 3.16. *Let S be a scheme and let A be an N-torsion commutative group scheme over S which sits in an extension*

$$0 \to \mu_N \to A \to \mathbf{Z}/N \to 0$$

of fppf sheaves of abelian groups. Let $\epsilon \in \mathrm{H}^1(S, \mu_N)$ be the image of 1 via the coboundary map $(\mathbf{Z}/N)(S) \to \mathrm{H}^1(S, \mu_N)$. Then, for any i, the map $\mathrm{H}^i(S, \mathbf{Z}/N) \to \mathrm{H}^{i+1}(S, \mu_N)$ is given by the cup product map

$$\epsilon \cup (-) \colon \mathrm{H}^i(S, \mathbf{Z}/N) \to \mathrm{H}^{i+1}(S, \mu_N).$$

Proof. Since A is N-torsion, the extension $0 \to \mu_N \to A \to \mathbf{Z}/N \to 0$ is determined by a homotopy class of maps $\mathbf{Z}/N \to \mu_N[1]$ in the derived category of fppf sheaves of $\mathbf{Z}/N$-modules. Since the constant sheaf $\mathbf{Z}/N$ is the unit object of this category, we have

$$\mathrm{Hom}_S(\mathbf{Z}/N, \mu_N[1]) \cong \mathrm{H}^1(S, \mu_N).$$

Now, giving a class $\chi \in \mathrm{H}^i(S, \mathbf{Z}/N)$ is equivalent to giving a homotopy class of maps $\mathbf{Z}/N \to \mathbf{Z}/N[i]$ in the derived category. We can compose with the suspension

$$\epsilon[i] \colon \mathbf{Z}/N[i] \to \mu_N[i+1]$$

to obtain the Yoneda/cup product

$$\mathbf{Z}/N \xrightarrow{\chi} \mathbf{Z}/N[i] \xrightarrow{u} \mu_N[i+1],$$

which is what we wanted to show. □

3.3 Splitting μ_N-gerbes with abelian scheme torsors

Recall the following theorem of Raynaud [6, Thm. 3.1.1].

Theorem 3.17 (Raynaud)**.** *Let $A \to S$ be a finite flat N-torsion commutative group scheme. Zariski locally on S there exists an abelian scheme $J \to S$ and an inclusion $A \to J[N]$.*

We use Raynaud's theorem to show that every μ_N-gerbe over a field is split by a torsor for an abelian variety.

Theorem 3.18. *Let k be a field. If $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N) \cong \mathrm{Br}(k)[N]$, then there exists an abelian scheme $J' \to \operatorname{Spec} k$ and a J'-torsor $X \to \operatorname{Spec} k$ such that β restricts to 0 in $\mathrm{H}^2(X, \mu_N)$.*

Proof. Let K be a finite étale extension of k which splits β. Denote by $p \colon \operatorname{Spec} K \to \operatorname{Spec} k$ the morphism of schemes and let $A = p_*\mu_N$, which is a finite flat group scheme on $\operatorname{Spec} k$. Geometrically, A is a direct sum of r copies of μ_N where r is the degree of K over k. There is a natural injective unit map $\mu_N \to A = p_*\mu_N$ and we let A' be the quotient. The Leray spectral sequence $\mathrm{E}_2^{s,t} = \mathrm{H}^s(\operatorname{Spec} k, \mathrm{R}p^t_*\mu_N) \Rightarrow \mathrm{H}^{s+t}(\operatorname{Spec} K, \mu_N)$ gives rise to an exact sequence of low degree terms

$$\mathrm{H}^1(\operatorname{Spec} k, \mu_N) \to \mathrm{H}^1(\operatorname{Spec} K, \mu_N) \to \mathrm{H}^0(\operatorname{Spec} k, \mathrm{R}p^1_*\mu_N) \to \mathrm{H}^2(\operatorname{Spec} k, \mu_N) \to \mathrm{H}^2(\operatorname{Spec} K, \mu_N),$$

which we see we can rewrite as part of the long exact sequence

$$\mathrm{H}^1(\operatorname{Spec} k, \mu_N) \to \mathrm{H}^1(\operatorname{Spec} k, A) \to \mathrm{H}^1(\operatorname{Spec} k, A') \xrightarrow{\delta} \mathrm{H}^2(\operatorname{Spec} k, \mu_N) \to \mathrm{H}^2(\operatorname{Spec} k, A)$$

in cohomology arising from the short exact sequence $0 \to \mu_N \to A \to A' \to 0$. Since β maps to 0 in $\mathrm{H}^2(\operatorname{Spec} k, A) \cong \mathrm{H}^2(\operatorname{Spec} K, \mu_N)$, there is some class $\sigma \in \mathrm{H}^1(\operatorname{Spec} k, A')$ such that $\delta(\sigma) = \beta$. Using Raynaud's theorem, fix an abelian scheme J together with an embedding $A \hookrightarrow J$. Let $J' = J/\mu_N$ where $\mu_N \subseteq A \subseteq J$. In this way, we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_N & \longrightarrow & A & \longrightarrow & A' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mu_N & \longrightarrow & J & \longrightarrow & J' & \longrightarrow & 0 \end{array}$$

of exact sequences. There is an associated commutative diagram

$$\begin{array}{ccc} \mathrm{H}^1(\operatorname{Spec} k, A') & \xrightarrow{\delta} & \mathrm{H}^2(\operatorname{Spec} k, \mu_N) \\ \downarrow & & \| \\ \mathrm{H}^1(S, J') & \xrightarrow{\delta} & \mathrm{H}^2(S, \mu_N) \end{array}$$

of boundary maps. If X_σ is the J'-torsor associated to $\sigma \in \mathrm{H}^1(\operatorname{Spec} k, A')$ via the left vertical map, then commutativity of the diagram implies that X splits $\delta(\sigma) = \beta$, as desired. □

Remark 3.19. The entire proof goes through with k replaced by a local ring R. Indeed, the only subtle point is the existence of a finite étale morphism $R \to R'$ such that β is split by R', which is proven in [5, Thm. 6.3].

3.4 Proof of Theorem A

Let E be an elliptic curve over a field k. As in Section 3.2, let $\varphi\colon E \to E'$ be a μ_N-isogeny. Then the short exact sequence (6) induces a boundary map $\mathrm{H}^1(\operatorname{Spec} k, \mathbf{Z}/N) \to \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$. By Lemma 3.16, this is given by taking the cup product with $\delta(P) \in \mathrm{H}^1(\operatorname{Spec} k, \mu_N)$ where $P \in E'(k)/NE'(k)$ and $\delta\colon E'(k)/NE'(k) \to \mathrm{H}^1(\operatorname{Spec} k, \mu_N)$. The homomorphism $\mathbf{Z}/N \to E'$ induced from the dual isogeny determines a map $\chi \mapsto X_\chi$ on cohomology $\mathrm{H}^1(\operatorname{Spec} k, \mathbf{Z}/N) \to \mathrm{H}^1(\operatorname{Spec} k, E')$.

Lemmas 3.14 and 3.15 show that the E'-torsor X_χ splits $\chi \cup \delta(P) = -\delta(P) \cup \chi$. We give in Figure 1 some discriminants of explicit families of elliptic curves, i.e., elliptic curves E defined over a rational function field $k(\lambda)$, with exact order N-points P together with a calculation of explicit elements in $k[\lambda]$ that represent $\delta(P) \in k(\lambda)^\times/k(\lambda)^{\times N}$. These families are all defined over $\mathbf{Z}$ away from the discriminant locus (except when $N = 2$ and we give two families) and they all admit points over fields of every characteristic (again, except for $N = 2$). Verification of these properties is given in Appendix A.

Proof of Theorem A. Assume that $N = 2, 3, 4$, or 5 and that $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$ is cyclic. Specifically, $\beta = \chi \cup u$ for some $\chi \in \mathrm{H}^1(\operatorname{Spec} k, \mathbf{Z}/N)$ and $u \in k^\times$ representing an element of $k^\times/(k^\times)^N \cong \mathrm{H}^1(\operatorname{Spec} k, \mu_N)$. We give the proof of the theorem in the $N = 5$ case; the proofs for $N = 2, 3$, and 4 are similar. The $N = 5$ line of Table 1 describes the discriminant and boundary value $\delta(P) \in \mathrm{H}^1(\operatorname{Spec} k, \mu_N)$ of a family of elliptic curves with a fixed 5-torsion point at $P = (0, 0)$. We claim that we can choose $\lambda \in k^\times$ such that

- λ and u generate the same subgroup of $k^\times/(k^\times)^5$ and
- $\Delta(\lambda) \neq 0$.

N	$\Delta(\lambda)$	$\delta(P)$
2, $p \neq 2$	$256\lambda^4 - 64\lambda^3$	λ
2, $p = 2$	λ^2	λ
3	$(1 - 27\lambda)\lambda^3$	λ^2
4	$-16\lambda^5 + \lambda^4$	λ^3
5	$\lambda^5(\lambda^2 - 11\lambda - 1)$	λ^4
6	$\lambda^6(\lambda - 1)^3(9\lambda - 1)$	$\lambda^5(\lambda - 1)^4$
7	$-\lambda^7(\lambda - 1)^7(\lambda^3 + 5\lambda^2 - 8\lambda + 1)$	$\lambda^6(\lambda - 1)^3$
8	$\lambda^8(\lambda - 1)^4(\lambda^2 - 6\lambda + 1)/(\lambda + 1)^{10}$	$\lambda^7(\lambda - 1)^6(\lambda + 1)^4$
9	$\lambda^9(\lambda + 1)^9(\lambda^2 + \lambda + 1)^3(\lambda^3 - 3\lambda^2 - 6\lambda - 1)$	$\lambda^8(\lambda + 1)^5(\lambda^2 + \lambda + 1)^6$
10	$\lambda^{10}(\lambda + 1)^{10}(2\lambda + 1)^5(4\lambda^2 + 6\lambda + 1)/(\lambda^2 - \lambda - 1)^{10}$	$\lambda^9(\lambda + 1)(2\lambda + 1)^8(\lambda^2 - \lambda - 1)^5$
12	$\lambda^{-24}(\lambda - 1)^{12}(2\lambda - 1)^6(3\lambda^2 - 3\lambda + 1)^4(2\lambda^2 - 2\lambda + 1)^3(6\lambda^2 - 6\lambda + 1)$	$-\lambda^{11}(\lambda - 1)^{11}(2\lambda - 1)^{10}(2\lambda^2 - 2\lambda + 1)^8(3\lambda^2 - 3\lambda + 1)^9$

Figure 1: The discriminants and boundary values $\delta(P)$ for various families of elliptic curves E' with exact order N points P. See the Appendix for the Weierstrass equations and details on the calculation.

We could let $\lambda = u$ to arrange for the first condition, but we have to check also that $\Delta(u) = u^5(u^2 - 11u - 1)$ is non-zero. Since u is a unit, this is equivalent to $u^2 - 11u - 1 \neq 0$ in k. However, of course, sometimes this will vanish for particular u. Any number of the form $\lambda = uv^5$ where $v \in k^\times$ will also satisfy the first condition. If k is infinite, this gives infinitely many possibilities for λ, at most 2 of which will have vanishing discriminant, so we can find some number of the form uv^5 such that $\Delta(uv^5) \neq 0$. If k is finite, then $\beta = 0$ and there is nothing to prove. In any case, letting $\lambda = uv^5$ be a choice which satisfies the two criteria above, we find by Lemmas 3.14 and 3.15 and by Figure 1 that X_χ splits $\chi \cup u^4$ and thus also $\chi \cup u$, as desired.

Now, fix $N = 6, 7, 8, 9, 10$, or 12 and assume that k is global. By the theorem of Albert–Brauer–Hasse–Noether ([10], [22], see for example [72, XIII.6], [51]), every $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$ is cyclic, of the form $\chi \cup u$ for some order N character χ and some unit u. Recall for instance from [65] the fundamental exact sequence of class field theory

$$0 \to \mathrm{Br}(k) \to \bigoplus_{\mathfrak{p}} \mathrm{Br}(k_\mathfrak{p}) \to \mathbf{Q}/\mathbf{Z} \to 0,$$

where the direct sum ranges over all places of k, both archimedean and non-archimedean. We claim we can find λ such that the field extension $k(\delta(P)^{1/N})$ splits β. Let S be the set of places $\mathfrak{p}$ in the support of β, i.e., where the associated Brauer class α is non-zero in $\mathrm{Br}(k_\mathfrak{p})$. By standard ramification theory, in order for $k(\delta(P)^{1/N})$ to split β, it is enough to find λ such that if $\mathfrak{p} \in S$ is finite, then $v_\mathfrak{p}(\delta(P))$ is a unit modulo N (where we normalize so that $v_\mathfrak{p}$ takes integer values) and if $\mathfrak{p} \in S$ is a real place (and without loss of generality N is even), then $\delta(P)$ is negative in the corresponding real embedding (since $\delta(P)$ is well-defined up to Nth powers, for even N the sign of $\delta(P)$ makes sense). For $N = 6, 7, 8, 9, 10$, or 12, since $v_\mathfrak{p}(\delta(P)) \equiv (N-1)v_\mathfrak{p}(\lambda) \pmod N$ it suffices to choose λ such that $v_\mathfrak{p}(\lambda)$ is a unit modulo N for each finite place $\mathfrak{p}$ in S. For any real place $\mathfrak{p}$ in S, it suffices to take: λ very negative for $N = 6, 8$, since $\delta(P)$ is an odd function with positive leading coefficient; $|\lambda - 1|_\mathfrak{p} < \frac{1}{2}$ for $N = 10$, since $\delta(P)$ is negative in that region; and λ very large for $N = 12$, since $\delta(P)$ is an even function with negative leading coefficient. By weak approximation, we can arrange for all of these conditions to be satisfied by some $\lambda \in k$.

It follows, in each of these cases, that $k(\delta(P)^{1/N})$ splits β. Now, results of Albert [1], Hochschild (see [20, Thm. 9.1.1]), Vishne [68], and Mináč–Wadsworth [43] imply (under the hypotheses of the theorem) that since β is split by $k(\delta(P)^{1/N})$ we have in fact $\beta = \chi' \cup \delta(P)$ for some character χ'. Specifically, if N is square-free, then we can use Albert's result to get χ'. If N is composite but prime to $\mathrm{char}(k)$, then we use the results of Vishne and Mináč–Wadsworth to deduce the existence of χ', under the assumptions of the theorem. If $N = 8, 9$ and $\mathrm{char}(k) = 2, 3$, respectively, then we can use Hochschild's result to produce χ'. Finally, if $N = 12$ and $\mathrm{char}(k) = 2$, then we use Hochschild's result for the existence of a degree 4 character

χ_4' such that $\chi_4' \cup \delta(P) = 3\chi \cup u \in \mathrm{H}^2(\operatorname{Spec} k, \mu_4)$ and we use Albert's theorem for the existence of a degree 3 character χ_3' such that $\chi_3' \cup \delta(P) = 4\chi \cup u \in \mathrm{H}^2(\operatorname{Spec} k, \mu_3)$. Thus, letting $\chi' = \chi_3' - \chi_4'$, we have that $\chi' \cup \delta(P) = \chi \cup u \in \mathrm{H}^2(\operatorname{Spec} k, \mu_1 2)$. In all of these cases, the curve $X_{\chi'}$ splits β, which is what we wanted to show. □

3.5 Proof of Theorem B

Proof of Theorem B. It is enough to know that under the conditions of the theorem, every class $\beta \in \mathrm{H}^2(\operatorname{Spec} k, \mu_N)$ is a sum of cyclic classes, for then we can split by a product of genus 1 curves using Theorem A. Using prime decomposition, we can separately handle $N = 2, 3, 4$, and 5. If the characteristic p of k is non-zero and divides N, then the result is due to Teichmüller; see [20, Thm. 9.1.4]. So, assume that p is prime to N. In this case, the fact results from Merkurjev's theorems [38, 39] when $N = 2$ or 3, from the Merkurjev–Suslin theorem [40] when $N = 4$ and k contains a primitive 4th root of unity, and from a theorem of Matzri [36] when $N = 5$. See [4, Section 3] for further discussion. □

3.6 Proof of Theorem C

We need the following easy lemma to begin.

Lemma 3.20. *Suppose that $Y \in \mathrm{H}^1(S, E[N])$ is an $E[N]$-torsor with $Ob_{\mathcal{L}}(Y) = \alpha \in \mathrm{H}^2(S, \mathbf{G}_m)$. If $X \in \mathrm{H}^1(S, E)$ is the E-torsor associated to Y, then X splits α.*

Proof. The group $E[N]$ acts on the flag $E[N] \subseteq E \subseteq \mathbf{P}(p_*\mathcal{L})$. Thus, to the $E[N]$-torsor Y, we get a twisted form P of $\mathbf{P}(p_*\mathcal{L})$, a Severi–Brauer scheme over S variety with Brauer class $\alpha = Ob_{\mathcal{L}}(Y)$, together with a flag of subvarieties $Y \subseteq X \subseteq P$ where X is the genus 1-curve associated to Y. Thus, X splits the class α. □

Note that Example 3.8 shows that in general X does not split the μ_N-gerbe β associated to α in the context of Lemma 3.20.

Proof of Theorem C. Fix k and E as in the statement of the theorem and fix a full level N structure $\varphi\colon E[N] \to \mathbf{Z}/N \times \mu_N$, which we can take to be symplectic since we are working over a field. Let P be the exact order N point $\varphi^{-1}(1 \times 1)$ and let $\mathcal{L} = \mathcal{O}(0_E + P + \cdots + (N-1)P)$. By Proposition 2.14, given an $E[N]$-torsor Y, which we can represent as a pair $\chi \in \mathrm{H}^1(\operatorname{Spec} k, \mathbf{Z}/n)$ and $u \in \mathrm{H}^1(\operatorname{Spec} k, \mu_N)$, the period-index obstruction class $Ob_{\mathcal{L}}(Y)$ is of the form $Ob_{\mathcal{L}}(Y) = [\chi + \sigma, u]$, where $\sigma \in \mathrm{H}^1(\operatorname{Spec} k, \mathbf{Z}/n)$ depends only on E, N, and ϕ. In particular, if Y corresponds to a pair $(\chi - \sigma, u)$, then $Ob_{\mathcal{L}}(Y) = [\chi, u]$. By Lemma 3.20, it follows that the E-torsor X corresponding to Y splits $[\chi, u]$, which completes the proof. □

A Fisher's method

Fisher [19] has developed a method to compute $\delta(P)$, as in Section 3.4, in the case of cyclic 5- and 7-isogenies. After some correspondence, Fisher provided a helpful explanation of his method, which we elaborate on here and carry out for $N = 4, \ldots, 10, 12$ using `MAGMA` and Sutherland's modular families [61, 60]. This is used to populate the table in Figure 1. Fisher's method works for $N \geqslant 4$, hence for $N = 2$ and $N = 3$, we must utilize other construction in the literature.

A.1 Computing the boundary

We recall the situation of Section 3.2. Fix an integer $N > 1$. Let E' be an elliptic curve over a field k with a rational point P of exact order N, which generates a subgroup $\mathbb{Z}/N \subseteq E'(k)$. Let $E' \xrightarrow{\phi'} E$ be the isogeny

whose kernel is this subgroup. The kernel of the dual isogeny $E \xrightarrow{\phi} E'$ is isomorphic to μ_N as a group scheme. We want to compute the boundary map in the exact sequence

$$0 \to \mu_N(k) \to E(k) \to E'(k) \xrightarrow{\delta} \mathrm{H}^1(\operatorname{Spec} k, \mu_N) \cong k^\times / k^{\times N}.$$

Lemma A.1. *There is a rational function f on E' and a rational function g on E such that $\operatorname{div}(f) = N(P) - N(0)$ and $f \circ \phi = g^N$.*

Proof. The existence of f follows from the fact that the divisor $N(P) - N(0)$ has degree 0 and has sum 0 in the group law on E. Now, let Q be an N-torsion lift of P to E, say over the algebraic closure. We have $\phi^*((P) - (0)) = \sum_{R \in \ker(\phi)}((Q + R) - (R))$, which is the divisor of some function g on E since $NQ = 0$. Now, $\operatorname{div}(f \circ \phi) = \operatorname{div}(g^N)$, so that after rescaling f by an element of $k^\times$, we can assume that $f \circ \phi = g^N$. □

Lemma A.2. *Let $N \geqslant 3$ and let f be a choice of rational function as in Lemma A.1. Suppose that $P' \in E'(k)$ is a point not equal to 0 or P, so that f has neither a zero nor pole at P'. Then, $\delta(P')$ and $f(P')$ generate the same subgroup of $k^\times / k^{\times N}$. If moreover $P' = aP$ for some integer $a \in \{2, \ldots, N-1\}$, then*

$$\delta(P') \equiv f(P')$$

in $k^\times / k^{\times N}$.

Proof. First, we prove that $\delta(P')$ and $f(P')$ generate the same subgroup of $k^\times/(k^\times)^N$. We can assume that N is a prime power and then assume that $N = p$, a prime, by suitably factoring the isogeny ϕ. The classes $\delta(P')$ and $f(P')$ in $\mathrm{H}^1(\operatorname{Spec} k, \mu_p) \cong k^\times / k^{\times N}$ correspond to μ_p-torsors U and V over $\operatorname{Spec} k$. These classes generate the same subgroup of $k^\times / k^{\times N}$ if and only if there is a k-isomorphism $U \to V$ (note that this k-isomorphism is μ_p-equivariant if and only if the classes are equal). It would be sufficient to have a k-morphism $U \to V$, which will then be an isomorphism since we are working with torsors for a prime order group. But, over U, the class $\delta(P')$ is zero, so that there is a lift along ϕ of $P'|_U$ to an element $Q' \in E(U)$. In this case, $f(P') = f(\phi(Q')) = g(Q')^N$, so that $f(P')$ is an Nth-power in the group of units of U. Thus V admits a U-point, in other words, there is a morphism $U \to V$. Therefore, $\delta(P') \equiv f(P')^l$ for some $l \in (\mathbf{Z}/N)^\times$.

Now, we show that $l \equiv 1$ in $(\mathbf{Z}/N)^\times$ when $P' = aP$. If N is invertible in k, then this follows from a cocycle proof given in Fisher [19, Lem. 1.4] or Silverman [59, Sec. III.8]. However, we can reduce to this case by lifting E (which is ordinary) to characteristic 0. Specifically, there is a p-complete, p-torsion-free discrete valuation ring R with residue field k (for example by [35, Thm. 29.1]) and a lift of E to R (lift a Weierstrass equation). The point P also lifts by Hensel's lemma (applied to the moduli stack $\mathcal{M}_1(N)$, which is a scheme) and the function f does too. If K denotes the fraction field of R, then we can compare $\delta(P')$ and $f(P')$ in the diagram $k^\times/(k^\times)^N \leftarrow R^\times/(R^\times)^N \hookrightarrow K^\times/(K^\times)^N$ to deduce that $\delta(P')$ and $f(P')$ agree by reduction to the N invertible case. □

In order to compute the coboundary using Lemma A.2, one must find the function f and check that it is normalized correctly, so that $f \circ \phi = g^N$. A completely general way to find the unnormalized function f is via Miller's algorithm, explained in [59, Sec. 11.8]. But, this is overkill for our present purposes, and we explain Fisher's method for finding the unnormalized function f, which can be implemented with a simple `MAGMA` script displayed in Figure 2.

Once a rational function f on E with the correct divisor $N(P) - N(0)$ has been found, one normalizes it as follows. Let uf be a 'correct' function, so that $(uf) \circ \phi = g^N$ for some rational function g on E. Here, u is a unit in the base field k. Since δ is a homomorphism, we can, for example, compute the difference between $f(4P)$ and $f(2P)^2$, at least for $N \gg 0$.

Specifically, it is enough to find uf up to Nth powers, which we do via the following lemma.

```
> K<la> := FunctionField(Rationals());
> E := EllipticCurve([1-la,-la,-la,0,0]);
> V,Vmap := RiemannRochSpace(5*Divisor(E!0) - 5*Divisor(E![0,0]));
> assert Dimension(V) eq 1;
> KE<x,y> := FunctionField(E);
> f := Vmap(V.1);
> print f;
(-x - 1)*y + x^2
```

Figure 2: Fisher's `MAGMA` code, applied in the case of $N = 5$ below.

Lemma A.3. *Fix an integer $N > 2$. Choose integers a, b, A, B such that the following hold:*

(a) $A + B \equiv 1 \pmod{N}$,

(b) $aA + bB \equiv 0 \pmod{N}$, *and*

(c) $a, b \neq 0, 1 \pmod{N}$.

Then,

$$u \equiv f(aP)^{-A} f(bP)^{-B} \pmod{k^{\times N}}.$$

Proof. We have

$$u^A f(aP)^A u^B f(bP)^B \equiv 1 \pmod{k^{\times N}}$$

by (b) and the fact that $n \mapsto (uf)(nP)$ for $n \neq 0, 1 \pmod{N}$ are the values of a homomorphism, so after re-arranging and using (a), we find the desired claim using Lemma A.2, which applies by (c). □

Example A.4. The lemma will not apply when $N = 2$ or $N = 3$ because no choice of integers a, b, A, B satisfies (a), (b), and (c) in those cases. We will need to argue via a different approach, which we do individually below. For $N = 4$, we can take $a = 3$, $A = 2$, $b = 2$, $B = -1$. For $N \geqslant 5$, we can take $a = 2$, $A = 2$, $b = 4$, $B = -1$.

A.2 Calculations

Overview

Each section below gives a family (two families for $N = 2$) of elliptic curves E' with an exact order N point P together with a calculation of $\delta(nP)$ for $n = 1, \ldots, N-1$. For $N \geqslant 4$ and $n = 2, \ldots, N-1$, these values are obtained by computing the normalized function f as described above, which we possibly rescale by an Nth power for notational convenience. Then, by writing $P = mP + nP$ where $m, n \in \{2, \ldots, N-1\}$ and using that $\delta(P) = \delta(mP)\delta(nP)$, we can fill in the final value $\delta(P)$ of the table. As N gets larger, the formulas are more complicated and we include less information. For $N = 2$ and $N = 3$, we refer instead to the literature for appropriate families and boundary map calculations. With the exception of the families at $N = 2$, the remainder work in all characteristics.

The reader may verify the calculations here for $N \geqslant 4$ by running `magma N-families.magma` with the attached `MAGMA` files, which computes the normalized function f and the values of f on $2P, \ldots, (N-1)P$. Note however that we have at times chosen to simplify the tables by changing the output of f by Nth powers.

$N = 2$

We use two families of elliptic curves E', i.e., elliptic curves over the rational function field $k(\lambda)$, depending on the characteristic of k. The first, when k has characteristic not 2, is the family

$$y^2 = x^3 - 4\lambda x^2 + \lambda x,$$

which has discriminant $\Delta(\lambda) = 256\lambda^4 - 64\lambda^3$ and a point $P = (0, 0)$ of exact order 2. Silverman gives

$$\delta(P) \equiv \lambda \pmod{k^{\times 2}}$$

in [59, Prop. X.4.9]. The second, when k has characteristic 2, is defined by

$$y^2 + xy = x^3 + x^2 + \lambda^2,$$

which has discriminant $\Delta(\lambda) = \lambda^2$ and a point $P = (0, \lambda)$ of exact order 2. Kramer gives

$$\delta(P) \equiv \lambda \pmod{k^{\times 2}}$$

in [29, Prop. 1.1(b)].

$N = 3$

Kozuma [28] studies the elliptic curve E'_λ over $k(\lambda)$ defined by

$$y^2 + xy + \lambda y = x^3$$

with an exact order 3 point $P = (0, 0)$. The discriminant of this Weierstrass equation is $\Delta(\lambda) = (1 - 27\lambda)\lambda^3$. Figure 3 shows the values of the boundary map at the multiples of P, which can be found in [28, Eq. 3.5].

The discriminant is not identically zero modulo any prime p, so this family and the corresponding calculation is available in all characteristics.

nP	(x_{nP}, y_{nP})	$\delta(nP)$
P	$(0, 0)$	λ^2
$2P$	$(0, -\lambda)$	λ

Figure 3: The coordinates of the multiples of P and the values of $\delta(nP)$ for $N = 3$.

$N = 4$

For $N \geqslant 4$ we will use families of elliptic curves in Tate normal form

$$y^2 + (1 - c)xy - by = x^3 - bx^2 \tag{7}$$

for values of $b, c \in k(\lambda)$. For $N = 4$, we take $c = 0$, as explained in [27, V.5 (5.31)], and set $b = -\lambda$ to get the elliptic curve

$$y^2 + xy + \lambda y = x^3 + \lambda x^2$$

over $k(\lambda)$, with a point of order 4 at $P = (0, 0)$ and discriminant $\Delta(\lambda) = -16\lambda^5 + \lambda^4$.

As an example of using Fisher's method, we start with the rational function $f(x, y) = y - x^2$ having the correct divisor. However, there is a normalization problem in this case. Indeed, we have $f(3P) = f(0, -\lambda) =$

$-\lambda$, which implies that we should set $f(P) = -\lambda^3$ (or $f(P) = -\frac{1}{\lambda}$). However, $f(2P) = f(-\lambda, 0) = -\lambda^2$ and we should have

$$\lambda^3 = f(2P)f(3P) \equiv f(P) = -\lambda^3,$$

which is typically false. So, following Fisher's algorithm, we can correct f by multiplying by -1. Having thus found $f = x^2 - y$, we can compute $\delta(2P) = f(2P)$ and $\delta(3P) = f(3P)$, which we can use to find $\delta(P) \equiv \delta(2P)\delta(3P) \pmod{k(\lambda)^{\times 4}}$.

nP	(x_{nP}, y_{nP})	$\delta(nP)$
P	$(0, 0)$	λ^3
$2P$	$(-\lambda, 0)$	λ^2
$3P$	$(0, -\lambda)$	λ

Figure 4: The coordinates of the multiples of P and the values of $\delta(nP)$ (equal to $f(nP)$ for $n = 2, 3$ where $f = x^2 - y$) for $N = 4$.

$N = 5$

We use the Tate normal form (7) with $b = c = \lambda$, as in [27, V.5 (5.31)], to get the elliptic curve

$$y^2 + (1 - \lambda)xy - \lambda y = x^3 - \lambda x^2$$

over $k(\lambda)$ with a point of order 5 point $P = (0, 0)$ and discriminant $\Delta(\lambda) = \lambda^7 - 11\lambda^6 - \lambda^5$, cf. [19]. Fisher's method produces the rational function $f(x, y) = -x^2 + xy + y$, which is already normalized (up to 5th powers).

nP	(x_{nP}, y_{nP})	$\delta(nP)$
P	$(0, 0)$	λ^4
$2P$	(λ, λ^2)	λ^3
$3P$	$(\lambda, 0)$	$-\lambda^2$
$4P$	$(0, \lambda)$	λ

Figure 5: The coordinates of the multiples of P and the values of $\delta(nP)$ (equal to $f(nP)$ for $n = 2, 3, 4$, where $f = -x^2 + xy + y$) for $N = 5$.

$N = 6$

For $N \geqslant 6$, we will utilize the Tate normal form (7), with the convention that

$$c = s(r - 1), \qquad b = rc \tag{8}$$

for elements $r, s \in k(\lambda)$, as in Sutherland [61, 60]. For $N = 6$, we use $r = 1 - \lambda$ and $s = 1$ giving the elliptic curve

$$y^2 + (1 + \lambda)xy - (\lambda - \lambda^2)y = x^3 - (\lambda - \lambda^2)x^2$$

over $k(\lambda)$ with an order 6 point $P = (0, 0)$ and discriminant $\Delta(\lambda) = \lambda^6(\lambda - 1)^3(9\lambda - 1)$.

nP	(x_{nP}, y_{nP})	$\delta(nP)$
P	$(0,0)$	$\lambda^5(\lambda-1)^4$
$2P$	$(\lambda(\lambda-1), -\lambda^2(\lambda-1))$	$\lambda^4(\lambda-1)^2$
$3P$	$(-\lambda, \lambda^2)$	λ^3
$4P$	$(\lambda(\lambda-1), 0)$	$\lambda^2(\lambda-1)^4$
$5P$	$(0, \lambda(\lambda-1))$	$\lambda(\lambda-1)^2$

Figure 6: The coordinates of the multiples of P and the values of $\delta(nP)$ (equal to $f(nP)$ for $n = 2, 3, 4, 5$, where $f = -2xy - (1-\lambda)y + x^3 + (1-\lambda)x^2)$ for $N = 6$.

$N = 7$

We use the Tate normal form (7) with convention (8) $r = s = 1 - \lambda$, to get the elliptic curve

$$y^2 + (1 + \lambda - \lambda^2)xy + \lambda(1-\lambda)^2 y = x^3 + \lambda(1-\lambda)^2 x^2$$

over $k(\lambda)$ with an order 7 point $P = (0,0)$ and discriminant $\Delta(\lambda) = -\lambda^7(\lambda-1)^7(\lambda^3 + 5\lambda^2 - 8\lambda + 1)$, cf. [19].

nP	(x_{nP}, y_{nP})	$\delta(nP)$
P	$(0,0)$	$\lambda^6(\lambda-1)^3$
$2P$	$(-\lambda(\lambda-1)^2, -\lambda^2(\lambda-1)^3)$	$\lambda^5(\lambda-1)^6$
$3P$	$(\lambda(\lambda-1), -\lambda^2(\lambda-1))$	$\lambda^4(\lambda-1)^2$
$4P$	$(\lambda(\lambda-1), \lambda^2(\lambda-1)^2)$	$-\lambda^3(\lambda-1)^5$
$5P$	$(-\lambda(\lambda-1)^2, 0)$	$\lambda^2(\lambda-1)^8$
$6P$	$(0, -\lambda(\lambda-1)^2)$	$\lambda(\lambda-1)^4$

Figure 7: The coordinates of the multiples of P and the values of $\delta(nP)$ (equal to $f(nP)$ for $n = 2, 3, 4, 5, 6$, where $f = -x^2y + (2\lambda - 3)xy - (\lambda-1)^2 y + \lambda x^3 + (\lambda-1)^2 x^2)$ for $N = 7$.

$N = 8$

We use the Tate normal form (7) with convention (8) $r = 1/(1+\lambda)$ and $s = 1 - \lambda$ yielding the elliptic curve

$$y^2 + \big(1 - \tfrac{\lambda(\lambda-1)}{\lambda+1}\big)xy - \tfrac{\lambda(\lambda-1)}{\lambda+1} y = x^3 - \tfrac{\lambda(\lambda-1)}{\lambda+1} x^2$$

over $k(\lambda)$ with an order 8 point $P = (0,0)$ and discriminant $\Delta(\lambda) = \lambda^8(\lambda-1)^4(\lambda^2 - 6\lambda + 1)/(\lambda+1)^{10}$, cf. [61, 60].

$N = 9$

We use the Tate normal form (7) with convention (8) $r = \lambda^2 + \lambda + 1$ and $s = \lambda + 1$ yielding an elliptic curve over $k(\lambda)$ with an order 9 point $P = (0,0)$ and discriminant

$$\Delta(\lambda) = \lambda^9(\lambda+1)^9(\lambda^2 + \lambda + 1)^3(\lambda^3 - 3\lambda^2 - 6\lambda - 1).$$

nP	(x_{nP}, y_{nP})	$\delta(nP)$
P	$(0,0)$	$\lambda^7(\lambda-1)^6(\lambda+1)^4$
$2P$	$(\lambda(\lambda-1)/(\lambda+1)^2, \lambda^2(\lambda-1)^2/(\lambda+1)^3)$	$\lambda^6(\lambda-1)^4$
$3P$	$(\lambda(\lambda-1)/(\lambda+1), -\lambda^2(\lambda-1)/(\lambda+1)^2)$	$\lambda^5(\lambda-1)^2(\lambda+1)^4$
$4P$	$(-\lambda/(\lambda+1)^2, \lambda^2/(\lambda+1)^3)$	λ^4
$5P$	$(\lambda(\lambda-1)/(\lambda+1), \lambda^2(\lambda-1)^2/(\lambda+1)^2)$	$\lambda^3(\lambda-1)^6(\lambda+1)^4$
$6P$	$(\lambda(\lambda-1)/(\lambda+1)^2, 0)$	$\lambda^2(\lambda-1)^4$
$7P$	$(0, \lambda(\lambda-1)/(\lambda+1)^2)$	$\lambda(\lambda-1)^2(\lambda+1)^4$

Figure 8: The value of $\delta(nP)$ for $N = 8$.

nP	(x_{nP}, y_{nP})	$\delta(nP)$
P	$(0,0)$	$\lambda^8(\lambda+1)^5(\lambda^2+\lambda+1)^6$
$2P$	$(\lambda(\lambda+1)^2(\lambda^2+\lambda+1), \lambda^2(\lambda+1)^4(\lambda^2+\lambda+1))$	$\lambda^7(\lambda+1)^{10}(\lambda^2+\lambda+1)^3$
$3P$	$(\lambda(\lambda+1)^2, \lambda^2(\lambda+1)^3)$	$-\lambda^6(\lambda+1)^6$
$4P$	$(\lambda(\lambda+1)(\lambda^2+\lambda+1), \lambda^2(\lambda+1)(\lambda^2+\lambda+1)^2)$	$\lambda^5(\lambda+1)^2(\lambda^2+\lambda+1)^6$
$5P$	$(\lambda(\lambda+1)(\lambda^2+\lambda+1), \lambda^2(\lambda+1)^2(\lambda^2+\lambda+1))$	$-\lambda^4(\lambda+1)^7(\lambda^2+\lambda+1)^3$
$6P$	$(\lambda(\lambda+1)^2, \lambda^2(\lambda+1)^4)$	$\lambda^3(\lambda+1)^3$
$7P$	$(\lambda(\lambda+1)^2(\lambda^2+\lambda+1), 0)$	$-\lambda^2(\lambda+1)^8(\lambda^2+\lambda+1)^6$
$8P$	$(0, \lambda(\lambda+1)^2(\lambda^2+\lambda+1))$	$\lambda(\lambda+1)^4(\lambda^2+\lambda+1)^3$

Figure 9: The values of $\delta(nP)$ for $N = 9$.

$N = 10$

We use the Tate normal form (7) with convention (8) $r = -(\lambda+1)^2/(\lambda^2-\lambda-1)$ and $s = \lambda+1$ yielding an elliptic curve over $k(\lambda)$ with an order 10 point $P = (0,0)$ and discriminant

$$\Delta(\lambda) = \lambda^{10}(\lambda+1)^{10}(2\lambda+1)^5(4\lambda^2+6\lambda+1)/(\lambda^2-\lambda-1)^{10}.$$

$N = 12$

We use the Tate normal form (7) with convention (8) $r = (2\lambda^2-2\lambda+1)/\lambda$ and $s = (3\lambda^2-3\lambda+1)/\lambda^2$ yielding an elliptic curve over $k(\lambda)$ with an order 12 point $P = (0,0)$ and discriminant

$$\Delta(\lambda) = \lambda^{-24}(\lambda-1)^{12}(2\lambda-1)^6(3\lambda^2-3\lambda+1)^4(2\lambda^2-2\lambda+1)^3(6\lambda^2-6\lambda+1).$$

References

[1] A. Adrian Albert, *On normal Kummer fields over a non-modular field*, Trans. Amer. Math. Soc. **36** (1934), no. 4, 885–892. MR 1501774 1, 3.4

[2] Michael Artin, *Brauer-Severi varieties*, Brauer groups in ring theory and algebraic geometry (Wilrijk, 1981), Lecture Notes in Math., vol. 917, Springer, Berlin, 1982, pp. 194–210. 1

[3] Asher Auel, *Algebras of composite degree split by genus one curves*, http://www.birs.ca/events/2015/5-day-workshops/15w5016/videos/watch/201509151021-Auel.html, 2015. 1

nP	$\delta(nP)$
P	$\lambda^9(\lambda+1)(2\lambda+1)^8(\lambda^2-\lambda-1)^5$
$2P$	$\lambda^8(\lambda+1)^2(2\lambda+1)^6$
$3P$	$\lambda^7(\lambda+1)^3(2\lambda+1)^4(\lambda^2-\lambda-1)^5$
$4P$	$\lambda^6(\lambda+1)^4(2\lambda+1)^2$
$5P$	$\lambda^5(\lambda+1)^5(\lambda^2-\lambda-1)^5$
$6P$	$\lambda^4(\lambda+1)^6(2\lambda+1)^8$
$7P$	$\lambda^3(\lambda+1)^7(2\lambda+1)^6(\lambda^2-\lambda-1)^5$
$8P$	$\lambda^2(\lambda+1)^8(2\lambda+1)^4$
$9P$	$\lambda(\lambda+1)^9(2\lambda+1)^2(\lambda^2-\lambda-1)^5$

Figure 10: The values of $\delta(nP)$ for $N = 10$.

nP	$\delta(nP)$
P	$-\lambda^{11}(\lambda-1)^{11}(2\lambda-1)^{10}(2\lambda^2-2\lambda+1)^8(3\lambda^2-3\lambda+1)^9$
$2P$	$\lambda^{10}(\lambda-1)^{10}(2\lambda-1)^8(2\lambda^2-2\lambda+1)^4(3\lambda^2-3\lambda+1)^6$
$3P$	$-\lambda^9(\lambda-1)^9(2\lambda-1)^6(3\lambda^2-3\lambda+1)^3$
$4P$	$\lambda^8(\lambda-1)^8(2\lambda-1)^4(2\lambda^2-2\lambda+1)^8$
$5P$	$-\lambda^7(\lambda-1)^7(2\lambda-1)^2(2\lambda^2-2\lambda+1)^4(3\lambda^2-3\lambda+1)^9$
$6P$	$\lambda^6(\lambda-1)^6(3\lambda^2-3\lambda+1)^6$
$7P$	$-\lambda^5(\lambda-1)^5(2\lambda-1)^{10}(2\lambda^2-2\lambda+1)^8(3\lambda^2-3\lambda+1)^3$
$8P$	$\lambda^4(\lambda-1)^4(2\lambda-1)^8(2\lambda^2-2\lambda+1)^4$
$9P$	$-\lambda^3(\lambda-1)^3(2\lambda-1)^6(3\lambda^2-3\lambda+1)^9$
$10P$	$\lambda^2(\lambda-1)^2(2\lambda-1)^4(2\lambda^2-2\lambda+1)^8(3\lambda^2-3\lambda+1)^6$
$11P$	$-\lambda(\lambda-1)(2\lambda-1)^2(2\lambda^2-2\lambda+1)^4(3\lambda^2-3\lambda+1)^3$

Figure 11: The values of $\delta(nP)$ for $N = 12$.

[4] Asher Auel, Eric Brussel, Skip Garibaldi, and Uzi Vishne, *Open problems in central simple algebras*, Transformation Groups **16** (2011), no. 1, 219–264. 3.5

[5] Maurice Auslander and Oscar Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409. MR 121392 3.19

[6] Pierre Berthelot, Lawrence Breen, and William Messing, *Théorie de Dieudonné cristalline. II*, Lecture Notes in Mathematics, vol. 930, Springer-Verlag, Berlin, 1982. MR 667344 2.1, 3.3

[7] Enrico Bombieri and David Mumford, *Enriques' classification of surfaces in char. p. II*, Complex analysis and algebraic geometry, a collection of papers dedicated to K. Kodaira (W. L. Jr Baily and T. Shioda, eds.), Iwanami Shoten, Tokyo, 1977, pp. 23–42. MR 0491719 3.1

[8] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990. MR 1045822 2.4

[9] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). 1

[10] Richard Brauer, Helmut Hasse, and Emme Noether, *Beweis eines Hauptsatzesin der Theorie der Algebren*, J. Reine Angew. Math. **167** (1932), 399–404. 3.4

[11] Mirela Ciperiani and Daniel Krashen, *Relative Brauer groups of genus 1 curves*, Israel J. Math. **192** (2012), no. 2, 921–949. MR 3009747 1, 2.1, 3.1, 3.5, 3.6

[12] Pete L. Clark, *The period-index problem in WC-groups. I. Elliptic curves*, J. Number Theory **114** (2005), no. 1, 193–208. MR 2163913 1, 2, 2.9, 2.4

[13] ———, *Some open problems*, 2008, https://web.archive.org/web/20130801040810/http://math.uga.edu/~pete/openquestions.html. 1, 1

[14] Pete L. Clark and Shahed Sharif, *Period, index and potential. III*, Algebra Number Theory **4** (2010), no. 2, 151–174. MR 2592017 3.8

[15] Aise Johan de Jong, *A result of gabber*, http://math.columbia.edu/~dejong/papers/2-gabber.pdf, 2003. 3.1

[16] Aise Johan de Jong and Wei Ho, *Genus one curves and Brauer-Severi varieties*, Math. Res. Lett. **19** (2012), no. 6, 1357–1359. MR 3091612 1

[17] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR 5125 III

[18] Richard Elman, Nikita Karpenko, and Alexander Merkurjev, *The algebraic and geometric theory of quadratic forms*, American Mathematical Society Colloquium Publications, vol. 56, American Mathematical Society, Providence, RI, 2008. 1

[19] Tom Fisher, *Some examples of 5 and 7 descent for elliptic curves over* **Q**, J. Eur. Math. Soc. (JEMS) **3** (2001), no. 2, 169–201. MR 1831874 A, A.1, A.2, A.2

[20] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR 2266528 1, III, IV, 2.3, 3.4, 3.5

[21] Ilseop Han, *Relative Brauer groups of function fields of curves of genus one*, Communications in Algebra **31** (2003), no. 9, 4301–4328. 3.5

[22] Helmut Hasse, *Die Struktur der R. Brauerschen Algebrenklassen-gruppe über einem algebraischen Zahlkörper. Insbesondere begründungdes Normenrestsymbols und die Herleitung des Reziprozitätsgesetzes mitnichtkommutativen Hilfsmitteln*, Math. Annalen **107** (1933), 731–760. 3.4

[23] Wei Ho and Max Lieblich, *Splitting Brauer classes using the universal Albanese*, to appear in L'Enseignement Mathématique, arXiv:1805.12566, 2018. 1

[24] Taira Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95. MR 229642 III

[25] Daniel Huybrechts, *Fourier-Mukai transforms in algebraic geometry*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, Oxford, 2006. 2.1

[26] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR 772569 3

[27] Anthony Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, 1992. 1, A.2, A.2

[28] Rintaro Kozuma, *A note on elliptic curves with a rational 3-torsion point*, Rocky Mountain J. Math. **40** (2010), no. 4, 1227–1255. MR 2718812 A.2

[29] Kenneth Kramer, *Two-descent for elliptic curves in characteristic two*, Trans. Amer. Math. Soc. **232** (1977), 279–295. MR 441977 A.2

[30] Daniel Krashen and Max Lieblich, *Index reduction for Brauer classes via stable sheaves*, Int. Math. Res. Not. IMRN (2008), no. 8, Art. ID rnn010, 31. MR 2428144 1

[31] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237. MR 434947 1

[32] Stephen Lichtenbaum, *The period-index problem for elliptic curves*, Amer. J. Math. **90** (1968), 1209–1223. MR 237506 1

[33] Max Lieblich, *Period and index in the Brauer group of an arithmetic surface*, J. Reine Angew. Math. **659** (2011), 1–41, With an appendix by Daniel Krashen. MR 2837009 2.3, 2.3, 2.4

[34] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2021. 3.5, 3.7, 3.1

[35] Hideyuki Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid. MR 1011461 A.1

[36] Eliyahu Matzri, *All dihedral division algebras of degree five are cyclic*, Proc. Amer. Math. Soc. **136** (2008), no. 6, 1925–1931. MR 2383498 1, 3.5

[37] Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), With an appendix by Mazur and M. Rapoport. MR 488287 3.8

[38] Alexander S. Merkurjev, *On the norm residue symbol of degree* 2, Dokl. Akad. Nauk SSSR **261** (1981), no. 3, 542–547. MR 638926 1, 3.5

[39] ———, *Brauer groups of fields*, Comm. Algebra **11** (1983), no. 22, 2611–2624. MR 733345 1, 3.5

[40] Alexander S. Merkurjev and Andrei A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 5, 1011–1046, 1135–1136. MR 675529 1, 3.5

[41] James S. Milne, *Weil-Châtelet groups over local fields*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 273–284. MR 276249 2.3

[42] ———, *Addendum: "Weil-Châtelet groups over local fields" (Ann. Sci. École Norm. Sup. (4)* **3** *(1970), 273–284)*, Ann. Sci. École Norm. Sup. (4) **5** (1972), 261–264. MR 327779 2.3

[43] Jan Mináč and Adrian Wadsworth, *Division algebras of prime degree and maximal Galois p-extensions*, Canad. J. Math. **59** (2007), no. 3, 658–672. MR 2319163 1, 3.4

[44] David Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354. MR 204427 2.4

[45] ———, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970. MR 0282985 2.1, 2.1, 2.4

[46] Andrew P. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. **12** (1971), 105–111. MR 291084 1

[47] Catherine O'Neil, *Jacobians of genus one curves*, Math. Res. Lett. **8** (2001), no. 1-2, 125–140. MR 1825265 2.4

[48] ———, *The period-index obstruction for elliptic curves*, J. Number Theory **95** (2002), no. 2, 329–339. MR 1924106 1, 2, 2.9, 2.4

[49] ———, *Erratum to âĂIJThe period-index obstruction for elliptic curves" [J. Number Theory 95 (2002) 329âĂŞ339]*, Journal of Number Theory **109** (2004), no. 2, 390. 2.4, 2.4

[50] Dimitri Orlov, Alexander Vishik, and Vladimir Voevodsky, *An exact sequence for* $K_*^M/2$ *with applications to quadratic forms*, Ann. of Math. (2) **165** (2007), no. 1, 1–13. 1

[51] Richard S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer-Verlag, New York-Berlin, 1982. MR 674652 3.4

[52] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of* $X(7)$ *and primitive solutions to* $x^2 + y^3 = z^7$, Duke Mathematical Journal **137** (2007), no. 1, 103–158. 2.4

[53] Peter Roquette, *Splitting of algebras by function fields of one variable*, Nagoya Math. J. **27** (1966), 625–642. MR 201435 1

[54] Anthony Ruozzi and Uzi Vishne, *Open problem session from the conference "Ramification in Algebra and Geometry at Emory"*, http://www.mathcs.emory.edu/RAGE/RAGE-open-problems.pdf, 2011. 1

[55] David J. Saltman, *Genus 1 curves in Severi–Brauer surfaces*, arXiv:2105.09986, 2021. 1

[56] Shahed Sharif, *Period and index of genus one curves over global fields*, Math. Ann. **354** (2012), no. 3, 1029–1047. MR 2983078 3.8

[57] Stephen S. Shatz, *The cohomology of certain elliptic curves over local and quasi-local fields*, Illinois J. Math. **11** (1967), 234–241. MR 215848 2.3

[58] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368 I

[59] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 2.4, 3.1, A.1, A.2

[60] Andrew V. Sutherland, *Optimized equations for $X_1(N)$*, https://math.mit.edu/~drew/X1_curves.txt. 1, A, A.2, A.2

[61] ———, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147. MR 2869053 1, A, A.2, A.2

[62] Paul Kenneth Swets, *Global sections of higher powers of the twisting sheaf on a Brauer-Severi variety*, ProQuest LLC, Ann Arbor, MI, 1995, Thesis (Ph.D.)–The University of Texas at Austin. MR 2693834 1

[63] John Tate, *WC-groups over p-adic fields*, Séminaire Bourbaki; 10e année: 1957/1958. Textes des conférences; Exposés 152 à 168; 2e éd. corrigée, Exposé 156, vol. 13, Secrétariat mathématique, Paris, 1958. MR 0105420 2.3

[64] ———, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR 206004 III

[65] ———, *Global class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 162–203. MR 0220697 3.4

[66] ———, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. Exp. No. 352, 95–110. MR 3077121 III

[67] ———, *A review of non-Archimedean elliptic functions*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 162–184. MR 1363501 3.1

[68] Uzi Vishne, *Galois cohomology of fields without roots of unity*, J. Algebra **279** (2004), no. 2, 451–492. MR 2078127 1, 3.4

[69] Vladimir Voevodsky, *Motivic cohomology with $\mathbf{Z}/2$-coefficients*, Publ. Math. Inst. Hautes Études Sci. (2003), no. 98, 59–104. 1

[70] ———, *Reduced power operations in motivic cohomology*, Publ. Math. Inst. Hautes Études Sci. (2003), no. 98, 1–57. MR 2031198 (2005b:14038a) 1

[71] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR 265369 III

[72] André Weil, *Basic number theory*, Springer, Berlin, Heidelberg, 1973. 3.4

[73] Yuri G. Zarhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15** (1974), 415–419. MR 354612 2.10, 2.4

Benjamin Antieau
Department of Mathematics
Northwestern University
2033 Sheridan Road
Evanston, IL 60208
antieau@northwestern.edu

Asher Auel
Department of Mathematics
Dartmouth College
6188 Kemeny Hall
Hanover, NH 03755
asher.auel@dartmouth.edu