GEOMETRIC DECOMPOSITION OF ABELIAN VARIETIES OF ORDER 1

TOREN D'NELLY-WARADY AND KIRAN S. KEDLAYA

Abstract. Since the 1970s, the complete classification (up to isogeny) of abelian varieties over finite fields with trivial group of rational points has been known from results of Madan–Pal and Robinson; with two exceptions these are all defined over $\mathbb{F}_2$. We determine the decomposition of these varieties into simple factors over an algebraic closure of $\mathbb{F}_2$; this requires solving a polynomial equation in three roots of unity.

1. Introduction

We say that an abelian variety A over a finite field $\mathbb{F}_q$ has *order* 1 if $\#A(\mathbb{F}_q) = 1$. The simple abelian varieties of order 1 were studied by Madan–Pal [12], who showed that there are none for $q \geq 5$, one isogeny class (of genus 1) for each of $q = 3$ and $q = 4$, and infinitely many isogeny classes for $q = 2$. More precisely, Madan–Pal produced a family of abelian varieties[1] A_n over $\mathbb{F}_2$ of order 1 with the property that every simple abelian variety over $\mathbb{F}_2$ of order 1 occurs as an isogeny factor of A_n for exactly one value of n. They also gave a partial analysis of the isogeny factors of the A_n, which was completed by Robinson [16]. We recall some more details in Theorem 4.1.

The main result of this paper is to determine how the simple abelian varieties over $\mathbb{F}_2$ of order 1 decompose into isogeny factors after base extension to an algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$. (See §8 for the proof.)

Theorem 1.1. *Let A be a simple abelian variety over $\mathbb{F}_2$ of order 1. Let n be the unique positive integer for which A is an isogeny factor of the Madan–Pal variety A_n. Then $A_{\overline{\mathbb{F}}_2}$ is isogenous to B^f for some simple abelian variety B over $\overline{\mathbb{F}}_2$, where*

$$f = \begin{cases} 1 & n \text{ is a power of } 2 \text{ and } n \neq 4 \\ 2 & n \text{ is not a power of } 2 \text{ and } n \neq 7, 30 \\ 2 & n = 4 \\ 3 & n = 7 \\ 4 & n = 30. \end{cases}$$

The main step between the Madan–Pal–Robinson classification and Theorem 1.1 is to identify ways that a ratio of two Frobenius eigenvalues can equal a nontrivial root of unity. This reduces to finding solutions to a certain polynomial equation in three roots of unity; to solve this problem, we apply the paradigm used by Kedlaya–Kolpakov–Poonen–Rubinstein [9] to classify tetrahedra with rational

D'Nelly-Warady was supported by the UC LEADS program. Kedlaya was supported by NSF (grants DMS-1802161, DMS-2053473) and UC San Diego (Warschawski Professorship).

[1]Note that the A_n are only specified by Madan–Pal up to isogeny, not up to isomorphism.

dihedral angles, incorporating two improvements. First, the classification of minimal additive relations among roots of unity has been extended from weight 12 (by Poonen–Rubinstein [15, Theorem 3.1]) to weight 20 (by Christie–Dykema–Klep [3, Theorem 4.3]; see Theorem 6.1). Second, the parallel classification of relations mod 2 has been extended from weight 12 (see [9, Theorem 6.8]) to weight 18 (see Theorem 6.4).

This analysis leaves a handful of exceptional cases, all involving abelian varieties of dimension at most 6. For these we may appeal directly to the L-Functions and Modular Forms Database (LMFDB) [11]: a single query returns all simple abelian varieties over $\mathbb{F}_2$ of order 1 of dimension at most 6, and we may simply look up the geometric decompositions of these.

As a byproduct, we also determine when two different abelian varieties in the Madan–Pal classification are geometrically isogenous to each other.

Corollary 1.2. *Let B_1, B_2 be simple abelian varieties over $\mathbb{F}_2$ of order 1. Then $\mathrm{Hom}(B_{1,\overline{\mathbb{F}}_q}, B_{2,\overline{\mathbb{F}}_q}) \neq 0$ if and only if either B_1 and B_2 are isogenous or there exists a pair (n_1, n_2) with*

$$\{n_1, n_2\} \in \{\{1,2\},\{1,4\},\{2,4\},\{3,30\},\{6,7\},\{7\},\{30\}\}$$

such that B_i is an isogeny factor of A_{n_i} for $i = 1, 2$.

It is natural to ask about other properties of simple abelian varieties of order 1; for instance, how often are they ordinary, or principally polarizable? We discuss some such questions in §9 and leave the rest to the interested reader.

Some of our arguments depend on computer calculations made in SageMath[17]. We have collected these in a series of Jupyter notebooks and made them available via a GitHub repository [5]. We also use the code accompanying [9] for computing torsion closures of ideals in Laurent polynomial ideals; see [10].

2. Weil polynomials

Throughout this section and the next, let $\mathbb{F}_q$ be a finite field of characteristic p. (We will eventually take $p = q = 2$, but we do not impose this restriction yet.)

By a *Weil polynomial* (or more precisely a *q-Weil polynomial* if we need to specify q), we will mean a monic integer polynomial $Q(x)$ of some even degree $2g$ such that every root of $Q(x)$ in $\mathbb{C}$ has absolute value $q^{1/2}$. Note that this implies that

$$Q(x) = \pm q^{-g} x^{2g} Q(q/x). \tag{2.0.1}$$

By a *real Weil polynomial*, we will mean a monic integer polynomial $R(x)$ with roots in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. For every real Weil polynomial, the formula

$$Q(x) = x^{\deg R(x)} R(x + qx^{-1}) \tag{2.0.2}$$

defines a Weil polynomial $Q(x)$; the Weil polynomials that occur in this way are precisely the ones for which the plus sign occurs in (2.0.1).

Now let A be an abelian variety over $\mathbb{F}_q$. By results of Weil, there is a Weil polynomial $Q(x)$ which equals the characteristic polynomial of Frobenius on the ℓ-adic Tate module for every prime ℓ not dividing q. Moreover, the plus sign occurs in (2.0.1), so we may associate to A both a Weil polynomial and a real Weil polynomial.

We say that A is *simple* if it is nonzero and not isogenous to the product of two nonzero abelian varieties. Since multiplication of Weil polynomials corresponds

to taking products of abelian varieties, any abelian variety with irreducible Weil polynomial is simple. The converse is not quite true because of the Honda–Tate theorem; see §3.

By the *Newton polygon* of A, we will mean the Newton polygon of its associated Weil polynomial $Q(x)$ with respect to the p-adic valuation v_q for the normalization $v_q(q) = 1$. It can also be computed from the Newton polygon of the real Weil polynomial $R(x)$ (for the same normalized valuation): by (2.0.2), all slopes in $[0, 1/2)$ have the same multiplicity in both polygons. (Explicitly, if $v_q(\alpha) \in [0, 1/2)$, then $v_q(q\alpha^{-1}) \in (1/2, 1]$ and so $v_q(\alpha + q\alpha^{-1}) = v_q(\alpha)$.) For each $s \in [0, 1)$, the multiplicity m_s of s as a slope in the Newton polygon has the property that $m_s s \in \mathbb{Z}$, e.g., from Manin's description of the formal group of A in terms of the quantities $m_s s$ [13, Theorem 4.1]; in other words, the Newton polygon of A has integral vertices. We say that A is *ordinary* if the slopes of its Newton polygon are all equal to 0 or 1.

For n a positive integer, let $A_{\mathbb{F}_{q^n}}$ denote the base extension of A from $\mathbb{F}_q$ to $\mathbb{F}_{q^n}$. From the definition of the Weil polynomial, we see that the Weil polynomial $Q_n(x)$ of $A_{\mathbb{F}_{q^n}}$ has roots which are the n-th powers of the roots of $Q(x)$; that is,

$$Q_n(x) = \mathrm{Res}_y(Q(y), y^n - x)$$

where Res denotes the resultant.

We say that A is *geometrically simple* if $A_{\mathbb{F}_{q^n}}$ is simple for each positive integer n, or equivalently if $A_{\overline{\mathbb{F}}_q}$ is simple.

Lemma 2.1. *Let A be a simple abelian variety over $\mathbb{F}_q$ with irreducible Weil polynomial $Q(x)$. If no two roots of $Q(x)$ have ratio equal to a nontrivial root of unity, then A is geometrically simple.*

Proof. Let $\pi \in \overline{\mathbb{Q}}$ be a root of $Q(x)$. Let f be the integer $[\mathbb{Q}(\pi) : \mathbb{Q}(\pi^n)]$. If $\pi_1, \dots, \pi_d$ are the conjugates of π listed without repetition, then $d = [\mathbb{Q}(\pi) : \mathbb{Q}]$; $\pi_1^n, \dots, \pi_d^n$ are the conjugates of π^n; and the number of distinct entries in this list is $[\mathbb{Q}(\pi^n) : \mathbb{Q}]$. It follows that $Q_n(x)$ is the f-th power of an irreducible polynomial.

In the above notation, the condition on $Q(x)$ implies that $f = 1$ for all n, so $Q_n(x)$ is irreducible for all n. □

Lemma 2.2. *Let A be an abelian variety over $\mathbb{F}_q$ of dimension $g > 2$ with Weil polynomial $Q(x)$. Suppose that the Newton polygon of A consists of the slopes $1/g$ and $1 - 1/g$, each with multiplicity g. Then A is geometrically simple.*

Proof. Since the condition on the Newton polygon is stable under base extension, it suffices to check that A is simple. For this, note that there is no way to separate the slopes of the Newton polygon into two sets of slopes which each satisfy the conditions on the Newton polygon of an abelian variety (namely, integer vertices and symmetry of slopes under $s \mapsto 1 - s$). □

3. The Honda–Tate theorem

We summarize [18, Theorem 8, Theorem 9].

Theorem 3.1 (Honda–Tate)**.** *There is a one-to-one correspondence between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and irreducible q-Weil polynomials, in which a simple abelian variety A corresponds to an irreducible q-Weil polynomial*

$Q(x)$ with the property that the Weil polynomial of A equals $Q(x)^e$ for some positive integer e. More precisely, e is the least common denominator of the following rational numbers indexed by places v of the number field $\mathbb{Q}(\pi) = \mathbb{Q}[x]/(Q(x))$:

- *If v is real:* $\frac{1}{2}$.
- *If v is complex:* 0.
- *If v lies over a finite prime not equal to p:* 0.
- *If v lies over p:* $\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)}[\mathbb{Q}(\pi)_v : \mathbb{Q}_p]$.

More precisely, the endomorphism algebra of A is a division algebra with center $\mathbb{Q}(\pi)$ and the listed quantities are the Brauer invariants of this division algebra.

Corollary 3.2. *For every simple abelian variety A over $\mathbb{F}_p$, the Weil polynomial of A is irreducible* unless *it equals $(x^2 - p)^2$.*

Proof. In Theorem 3.1, the invariant associated to every place above p is an integer (namely the degree of the residue field of $\mathbb{Q}(\pi)_v$ over $\mathbb{F}_p$). Hence the only way to get a nontrivial denominator is for $\mathbb{Q}(\pi)$ to have a real place, which occurs if and only if $Q(x) = x^2 - p$. □

Corollary 3.3. *For every* ordinary *simple abelian variety A over $\mathbb{F}_q$, the Weil polynomial of A is irreducible.*

Proof. In Theorem 3.1, the invariant associated to every place above p is an integer because $\mathrm{ord}_v(\pi)/\mathrm{ord}_v(q) \in \{0, 1\}$. Hence the only way to get a nontrivial denominator is for $\mathbb{Q}(\pi)$ to have a real place, which occurs if and only if $Q(x) = x^2 - q$ or $Q(x) = x \pm \sqrt{q}$; but these cases are not ordinary. □

4. The Madan–Pal–Robinson classification

We describe the classification of abelian varieties over $\mathbb{F}_2$ of order 1 in terms of their associated real Weil polynomials. This is due to Madan–Pal [12] modulo the computation of certain irreducible factors, which was completed by Robinson [16].

For n a positive integer, define the integer polynomial

$$P_n(x) = \prod_{0 \le k \le n/2, \gcd(n,k)=1} \left(x^2 - (4 + 2\cos\frac{2\pi k}{n})x + 1 \right) \tag{4.0.1}$$

of degree $\max\{2, \phi(n)\}$. For $n = 2, 7, 30$, $P_n(x)$ is reducible:

$$\begin{aligned} P_2(x) &= (x-1)^2 \\ P_7(x) &= (x^3 - 5x^2 + 6x - 1)(x^3 - 6x^2 + 5x - 1) \\ P_{30}(x) &= (x^4 - 8x^3 + 14x^2 - 7x + 1)(x^4 - 7x^3 + 14x^2 - 8x + 1). \end{aligned}$$

Theorem 4.1 (Madan–Pal, Robinson)**.** *The real Weil polynomials associated to simple abelian varieties over $\mathbb{F}_2$ of order 1 are precisely those of the form $P(3 - x)$ where $P(x)$ equals either $P_n(x)$ for some positive integer $n \neq 2, 7, 30$ or an irreducible factor of one of $P_2(x), P_7(x), P_{30}(x)$.*

Proof. We first check that Corollary 3.2 applies to show that $P_n(3 - x)$ is the real Weil polynomial of some abelian variety A_n over $\mathbb{F}_2$ of order 1. For this it suffices to verify that $x^2 - 2$ never occurs as a factor of $P_n(3 - x)$, or equivalently that $(3-x)^2 - 2 = x^2 - 6x + 7$ never occurs as a factor of $P_n(x)$; this is apparent because $P_n(0) = 1$.

By [12, Theorem 4], every simple abelian variety over $\mathbb{F}_2$ of order 1 is a factor of A_n for a unique value of n. It thus remains to compute the factorizations of the polynomials $P_n(x)$; this is established in [16] based on partial results from [12]. □

We next compute the Newton polygons of these abelian varieties.

Lemma 4.2. *For $n = 2^m$ with $m \geq 2$, $P_n(1) = (-1)^{n/4}2$.*

Proof. Let ζ be a primitive n-th root of unity. We may then write

$$\begin{aligned} P_n(1) &= \prod_{0 \leq k \leq n/2, \gcd(n,k)=1} \left(-2 - 2\cos\frac{2\pi k}{n}\right) \\ &= (-1)^{n/4} \prod_{0 \leq k \leq n/2, \gcd(n,k)=1} (2 + \zeta^k + \zeta^{-k}) \\ &= (-1)^{n/4} \prod_{0 \leq k \leq n/2, \gcd(n,k)=1} (1 + \zeta^k)(1 + \zeta^{-k}) \\ &= (-1)^{n/4} \Phi_n(-1) \end{aligned}$$

where $\Phi_n(x) = x^{n/2}+1$ is the n-th cyclotomic polynomial. Since evidently $\Phi_n(-1) = 2$, this proves the claim. □

Lemma 4.3. *Let A_n be the abelian variety with real Weil polynomial $P_n(3-x)$.*

(a) *If n is not a power of 2, then A_n is ordinary.*
(b) *If n is a power of 2, then the Newton polygon of A_n has all slopes equal to $1/2^m$ or $1 - 1/2^m$ where $m = \max\{1, \log_2(n) - 1\}$.*

Proof. Write $n = 2^m j$ with j odd. Over the ring of algebraic integers, (4.0.1) implies

$$P_n(x) \equiv \prod_{0 \leq k \leq n/2, \gcd(n,k)=1} \left(x^2 - (2\cos\frac{2\pi k}{n})x + 1\right) \equiv \Phi_n(x) \pmod 2; \tag{4.3.1}$$

in particular, each root of $P_n(x)$ is congruent modulo a prime above 2 to a primitive j-th root of unity. In case (a), this implies that none of the roots of $P_n(3-x)$ have positive valuation, as each root is congruent modulo a prime above 2 to $1-\eta$ where η is a primitive j-th root of unity for some $j > 1$; consequently, A_n is ordinary. In case (b), it implies that all of the roots of $P_n(3-x)$ have positive valuation; this automatically implies the claim for $m = 0, 1$. For $m \geq 2$, we also need to know that $P_n(3) \equiv 2 \pmod 4$ in order to deduce that $P_n(3-x)$ is an Eisenstein polynomial at 2; this follows by applying Lemma 4.2 and (4.3.1) to obtain

$$P_n(3) \equiv P_n(1) + 2P_n'(1) \equiv P_n(1) + 2\Phi_n'(1) \equiv 2 \pmod 4.$$ □

5. Reduction to an equation in roots of unity

Let A_n be an abelian variety over $\mathbb{F}_2$ with real Weil polynomial $P_n(3-x)$. In light of Lemma 2.1, the key step in the proof of Theorem 1.1 will be to determine when the ratio of two Frobenius eigenvalues of A_n can equal a nontrivial root of unity. The following lemmas reduce this to a tractable problem, which we solve in the remainder of the paper.

Lemma 5.1. *For any positive integer n, the Frobenius eigenvalues of A_n are precisely the numbers α satisfying an equation of the form*

$$\alpha - 2\eta\alpha^{-1} + \eta - 1 = 0 \tag{5.1.1}$$

for some primitive n-th root of unity η.

Proof. By definition, α is a Frobenius eigenvalue of A_n if and only if $\alpha + 2\alpha^{-1}$ is a root of the real Weil polynomial $P_n(3-x)$. From (4.0.1), the latter condition means that there exists a primitive n-th root of unity η such that

$$(3 - \alpha - 2\alpha^{-1}) + (3 - \alpha - 2\alpha^{-1})^{-1} = 4 + \eta + \eta^{-1}.$$

This equation simplifies to

$$(\alpha - 2\eta\alpha^{-1} + \eta - 1)(\alpha - 2\eta^{-1}\alpha^{-1} + \eta^{-1} - 1) = 0,$$

and so holds if and only if one of the two factors on the left vanishes. If it is the first factor, then (5.1.1) holds; otherwise, (5.1.1) becomes true after we replace η with η^{-1}. □

Lemma 5.2. *Let α_1, α_2 be distinct Frobenius eigenvalues of A_n. If $\eta_3 = \alpha_1/\alpha_2$ is a root of unity (of any order), then there exist roots of unity η_1, η_2 of order n such that $g(\eta_1, \eta_2, \eta_3) = 0$, where*

(5.2.1)

$$\begin{aligned} g(z_1, z_2, z_3) = {} & z_1 + z_1^{-1} + z_2 + z_2^{-1} \\ & + z_3 + z_3^{-1} - z_1 z_3^{-1} - z_1^{-1} z_3 - z_2 z_3^{-1} - z_2^{-1} z_3 + z_1 z_2 z_3^{-1} + z_1^{-1} z_2^{-1} z_3 \\ & - 2 z_1 z_2 z_3^{-2} - 2 z_1^{-1} z_2^{-1} z_3^2 \end{aligned}$$

as an element of the Laurent polynomial ring $R = \mathbb{Z}[z_1^{\pm}, z_2^{\pm}, z_3^{\pm}]$.

Proof. By Lemma 5.1, there exist roots of unity η_1, η_2 of order n such that

$$\alpha_1 - 2\eta_1\alpha_1^{-1} + \eta_1 - 1 = \alpha_2 - 2\eta_2^{-1}\alpha_2^{-1} + \eta_2^{-1} - 1 = 0.$$

We obtain (5.2.1) by substituting $\alpha_1 = \alpha_2\eta_3$ in the first equation to obtain

$$\begin{aligned} 0 &= \alpha_2^2\eta_3^2 + \alpha_2\eta_3(\eta_1 - 1) - 2\eta_1 \\ 0 &= \alpha_2^2 + \alpha_2(\eta_2^{-1} - 1) - 2\eta_2^{-1}, \end{aligned}$$

then eliminating α_2. This is an easy resultant computation in SageMath but can also be done by hand: subtract η_3^2 times the second equation from the first to obtain

$$(\eta_3 + \eta_2^{-1}\eta_3^2 - \eta_3^2 - \eta_1\eta_3)\alpha_2 = 2\eta_2^{-1}\eta_3^2 - 2\eta_1,$$

then substitute for α_2. □

6. Additive relations among roots of unity

Our approach to solving the equation $g(\eta_1, \eta_2, \eta_3) = 0$ from Lemma 5.2 is to treat it as an additive relation among 16 roots of unity. A strategy for analyzing such relations was described by Conway–Jones [4] and used thereafter by numerous authors; a recent example is [9], whose notation and terminology we follow (with some improvements as noted in the introduction).

Let μ be the multiplicative group of roots of unity in $\mathbb{C}$ and let $\mathbb{Z}[\mu] \subset \mathbb{C}$ be the ring of cyclotomic integers. For N a positive integer, let μ_N be the subgroup of μ generated by $\zeta_N = e^{2\pi i/N}$. By a *cyclotomic relation*, we will mean a multisubset

(subset with multiplicity) of μ with sum zero; this corresponds to the notion of a *sorou* (acronym for *sum of roots of unity*) in [3]. By a *mod* 2 *cyclotomic relation*, we will mean a multisubset of μ with sum divisible by 2 in $\mathbb{Z}[\mu]$.

A cyclotomic relation (resp. a mod 2 cyclotomic relation) is *indecomposable* if it is nonempty and cannot be partitioned into two nonempty cyclotomic relations (resp. mod 2 cyclotomic relations). The cardinality of a cyclotomic relation (resp. a mod 2 cyclotomic relation) is also called its *weight*.

Theorem 6.1. *Every indecomposable cyclotomic relation of weight at most* 20 *is a subset of* μ*; that is, its elements are pairwise distinct. (The bound is best possible; see Remark 6.5.)*

Proof. This follows from the explicit classification of minimal cyclotomic relations of weight at most 20 [3, Theorem 4.3]. For the case of weight at most 12, see also [15, Theorem 3.1]. □

For smaller weight, we will also need the explicit forms of such sequences.

Theorem 6.2. *Let* S *be an indecomposable cyclotomic relation of weight at most* 8*. Then then there exists* $\zeta \in \mu$ *such that* $\zeta^{-1}S = \{\zeta^{-1}\eta : \eta \in S\}$ *appears in Table 1.*

n	Type	Relation
2	R_2	$1, -1$
3	R_3	$1, \zeta_3, \zeta_3^2$
5	R_5	$1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$
6	$(R_5 : R_3)$	$\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4, -\zeta_3, -\zeta_3^2$
7	R_7	$1, \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6$
7	$(R_5 : 2R_3)$	$1, \zeta_5^2, \zeta_5^3, -\zeta_3\zeta_5, -\zeta_3^2\zeta_5, -\zeta_3\zeta_5^4, -\zeta_3^2\zeta_5^4$
7	$(R_5 : 2R_3)$	$1, \zeta_5, \zeta_5^4, -\zeta_3\zeta_5^2, -\zeta_3^2\zeta_5^2, -\zeta_3\zeta_5^3, -\zeta_3^2\zeta_5^3$
8	$(R_5 : 3R_3)$	$\zeta_5^2, \zeta_5^3, -\zeta_3, -\zeta_3^2, -\zeta_3\zeta_5, -\zeta_3^2\zeta_5, -\zeta_3\zeta_5^4, -\zeta_3^2\zeta_5^4$
8	$(R_5 : 3R_3)$	$\zeta_5, \zeta_5^4, -\zeta_3, -\zeta_3^2, -\zeta_3\zeta_5^2, -\zeta_3^2\zeta_5^2, -\zeta_3\zeta_5^3, -\zeta_3^2\zeta_5^3$
8	$(R_7 : R_3)$	$\zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6, -\zeta_3, -\zeta_3^2$

TABLE 1. Indecomposable cyclotomic relations of weight at most 8.

Proof. The result is originally due to Włodarski [19] and was extended to weight 9 by Conway–Jones [4]. Our notation follows [15, Table 3.1]. □

In many cases, one is particularly interested in cyclotomic relations which are stable under complex conjugation. Any such relation can be partitioned into indecomposable relations, but not uniquely; hence it is not automatic that there is such a partition which is stable under complex conjugation. We first address this question in the easier mod 2 setting, recalling [9, Lemma 6.9]; see Lemma 6.7 for an analogous statement for genuine cyclotomic relations.

Lemma 6.3. *Let* S *be a mod* 2 *cyclotomic relation (of any weight) which is stable under complex conjugation. Then* S *can be partitioned into indecomposable mod* 2 *cyclotomic relations in a manner which is itself stable under complex conjugation; that is, the conjugate of each part is also a part.*

Proof. We induct on the weight of S. Let T be an indecomposable mod 2 cyclotomic relation contained in S. Let $\overline{T}$ be the complex conjugate of T. If either $T = \overline{T}$ or $T \cap \overline{T} = \emptyset$, we apply the induction hypothesis to the complement of $T \cup \overline{T}$ in S; otherwise, we apply it to the symmetric difference $T \oplus \overline{T}$ and to its complement in S. □

The following is an extension of [9, Theorem 6.7, Corollary 6.8]. The bound is best possible; see again Remark 6.5.

Theorem 6.4. *Let $S = \{\eta_1, \dots, \eta_m\}$ be a mod 2 cyclotomic relation of weight at most 18. Then there exist signs $\sigma_1, \dots, \sigma_m \in \{\pm 1\}$ such that $\sigma_1\eta_1 + \cdots + \sigma_m\eta_m = 0$; that is, S can be "lifted" to a cyclotomic relation.*

Proof. We proceed by induction on m, using [9, Theorem 6.7] to treat the cases $m \leq 12$ as base cases. For the induction step, we may assume that S is indecomposable and $m \geq 13$. Let N be the *level* of S in the sense of [9, §6], i.e., the smallest positive integer for which $S \subseteq \mu_N$. We may assume that S is *minimal* in the sense that no rotation of S (i.e., the product of S with a root of unity) has level strictly less than N; in this case N is odd and squarefree [9, Lemma 6.1]. Let p be the largest prime factor of N; since $m > 10$ we must have $p \geq 7$. We can write S as a disjoint union $\bigsqcup_{i=0}^{p-1} \zeta_p^i T_i$ where T_i is a nonempty set of roots of unity whose orders are not divisible by p; the sums of the T_i are pairwise congruent modulo 2 (see the proof of [9, Lemma 6.4]).

If some T_i is empty, then each T_i is itself a mod 2 cyclotomic relation; this gives a contradiction against either the hypothesis that S is indecomposable (if there is more than one nonempty T_i) or the definition of the level (if only one T_i is nonempty).

If some T_i is a singleton, we may assume without loss of generality that $T_0 = \{1\}$. Then for each $i > 0$, $T_i \cup \{1\}$ is itself a mod 2 cyclotomic relation of weight at most $n - p + 1 < n$, so by the induction hypothesis we can find a function $f_i : T_i \to \{\pm 1\}$ such that

$$1 + \sum_{\eta \in T_i} f_i(\eta)\eta = 0.$$

Combining these, we obtain a lift of S to a cyclotomic relation.

We may thus assume that $\#T_i \geq 2$ for each i. This rules out $p \geq 11$, as this would imply $m \geq \sum_i \#T_i \geq 22$; we thus have $p = 7$. We also must have $\#T_i \leq 6$ for each i, as otherwise $m \geq \sum_i \#T_i \geq 7 + 6 \times 2 = 21$. We may assume without loss of generality that $T_0 = \{1, \zeta_N\}$ where $N \in \{3, 5, 15\}$. Then each T_i consists of powers of ζ_{15}, has sum congruent to $1 + \zeta_N$ mod 2, and contains no mod 2 cyclotomic relation; it is straightforward to enumerate all sets satisfying these conditions (of cardinality at most 6) using SageMath.

It now suffices to show that there exist functions $f_i : T_i \to \{\pm 1\}$ for $i = 1, \dots, 6$ such that the sums $\sum_{\eta \in T_i} f_i(\eta)\eta$ are either all equal to $1 + \zeta_N$ or all equal to $1 - \zeta_N$. From the enumeration, we see that for $N \in \{3, 5\}$, we can always achieve $\sum_{\eta \in T_i} f_i(\eta)\eta = 1 + \zeta_N$. When $N = 15$, there do exist indices $i \neq j \in \{1, \dots, 6\}$ such that for any functions $f_i : T_i \to \{\pm 1\}$, $f_j : T_j \to \{\pm 1\}$,

$$\sum_{\eta \in T_i} f_i(\eta)\eta \neq 1 + \zeta_N, \qquad \sum_{\eta \in T_j} f_j(\eta)\eta \neq 1 - \zeta_N;$$

however, for all such indices we have

$$\#T_i \geq 5, \qquad \#T_j \geq 4$$

and this cannot occur when $n \leq 18$. □

Remark 6.5. In [3, §2.2], an example is given of an indecomposable cyclotomic relation of weight 21 with one pair of repeated elements. Omitting this pair gives a mod 2 cyclotomic relation of weight 19 which cannot be lifted to a cyclotomic relation; one can extend the proof of Theorem 6.4 to give a complete classification of such relations.

Remark 6.6. In Theorem 6.4, if S is indecomposable (mod 2), then the choice of the σ_i is unique up to multiplying them all by -1, by the following reasoning. Suppose that $\sigma'_1, \dots, \sigma'_m \in \{\pm 1\}$ is a second choice for which $\sum_i \sigma'_i \eta_i = 0$. Define the partition $\{1, \dots, m\} = J_1 \sqcup J_2$ by

$$J_1 = \{i \in \{1, \dots, m\} : \sigma_i = \sigma'_i\}, \qquad J_2 = \{i \in \{1, \dots, m\} : \sigma_i \neq \sigma'_i\};$$

Then both $\{\sigma_i \eta_i : i \in J_1\}$ and $\{\sigma_i \eta_i : i \in J_2\}$ are cyclotomic relations, and hence mod 2 cyclotomic relations. Since S is indecomposable as a mod 2 cyclotomic relation, this is only possible if $J_1 = \emptyset$ or $J_2 = \emptyset$.

The following is an extension of [15, Lemma 4.1], but with a different proof. See also Remark 6.8.

Lemma 6.7. *Let S be a cyclotomic relation of weight at most 18 which is stable under complex conjugation. Then S can be partitioned into indecomposable cyclotomic relations in a manner which is itself stable under complex conjugation; that is, the conjugate of each part is also a part.*

Proof. We induct on the weight of S. By Lemma 6.3 S admits a conjugation-stable partition as a mod 2 cyclotomic relation. Apply Theorem 6.4 to lift each part to a genuine cyclotomic relation; by Remark 6.6 each of these lifts is unique up to an overall sign, so we can ensure that conjugate parts lift to conjugate relations.

This yields a conjugation-equivariant function $f : S \to \{\pm 1\}$ such that $\sum_{\eta \in S} f(\eta)\eta = 0$. If f is constant, we have a partition of S of the desired form; otherwise as in Remark 6.6 the level sets of f partition S nontrivially into two cyclotomic relations, each stable under complex conjugation. □

Remark 6.8. In this paper, we will only need Lemma 6.7 for weight at most 16. We describe an alternate proof of this restricted result in the style of the original proof of [15, Lemma 4.1].

Let T be an indecomposable cyclotomic relation of minimal weight contained in S. Let $\overline{T}$ be the complex conjugate of T; it will suffice to check that either $T = \overline{T}$ or $T \cap \overline{T} = \emptyset$, as then we can remove $T \cup \overline{T}$ from S and then apply the induction hypothesis to conclude.

If T is of type R_p for some prime p in the sense of Table 1 (i.e., a collection of p equally spaced roots of unity), then $\overline{T}$ is a rotation of T and so the claim is evident. In particular, this covers all cases where T has weight at most 5; since S has weight at most 17, this also covers all cases where S can be partitioned into three or more indecomposable cyclotomic relations.

The remaining case is where the complement T' of T in S is itself an indecomposable cyclotomic relation and both T and T' have weights in the range $\{6, 7, 8\}$.

By Theorem 6.2, there exists $\zeta \in \mu$ such that $\zeta^{-1}T$ is listed in Table 1. Since $T \cap \overline{T} \neq \emptyset$, there must be two (not necessarily distinct) entries η_i, η_j in the listed sequence such that $\zeta\eta_i = (\zeta\eta_j)^{-1}$, yielding

$$\zeta^2 = \eta_i^{-1}\eta_j^{-1}.$$

This limits T to a computable finite list of options, and similarly for T'.

Write T as the disjoint union of T_1 and T_2 where $T_1 = T \cap \overline{T}$, and similarly for T'. Then each of T_2 and T_2' is disjoint from its complex conjugate, and yet together they are stable under complex conjugation; they must therefore be conjugates of each other. In particular,

$$\sum T_1 = -\sum T_2 = \overline{-\sum T_2'} = \overline{\sum T_1'} = \sum T_1'.$$

We may thus check the claim by enumerating the candidates for T; for each T, computing the partition $T_1 \sqcup T_2$ and the sum $t = \sum T_1$; finding pairs $T \neq T'$ with matching values of t; and checking that for each such pair, the union $T \cup T'$ contains a cyclotomic relation which is either stable under complex conjugation or disjoint from its complex conjugate. This computation takes a few minutes in SageMath.

Remark 6.9. For $\eta_1, \eta_2 \in \mu$, if $\eta_1 - \eta_2$ has 2-adic valuation greater than 1 with respect to some prime above 2 in $\mathbb{Z}[\mu]$, then $\eta_1 = \eta_2$. To see this, suppose by way of contradiction that η_1/η_2 has order $m > 1$. If $m = \ell^e$ for some prime ℓ and some positive integer e, then by [8, Theorem 10.1] the 2-adic valuation of $\eta_1 - \eta_2$ is 0 if $\ell \neq 2$ or $1/\phi(m) \leq 1$ if $\ell = 2$. Otherwise, $\eta_1 - \eta_2$ is a unit in $\mathbb{Z}[\mu]$ [8, §I.10, Exercise 2].

If instead $\eta_1 - \eta_2$ has 2-adic valuation greater than $1/2^n$ for some positive integer n, then $\eta_1^2 - \eta_2^2 = (\eta_1 - \eta_2)(\eta_1 - \eta_2 + 2\eta_2)$ has 2-adic valuation at least $1/2^{n-1}$. By induction, we deduce that $\eta_1^{2^n} = \eta_2^{2^n}$.

7. Solving an equation in roots of unity

We now apply the results from §6, plus the computation of torsion closures described in [9, §7], to solve the equation $g(\eta_1, \eta_2, \eta_3) = 0$ from Lemma 5.2.

We first note that g is invariant under the group G generated by the substitutions

$$(z_1, z_2, z_3) \mapsto (z_1^{-1}, z_2^{-1}, z_3^{-1}), (z_2, z_1, z_3), (z_1, z_2^{-1}, -z_1/z_3). \tag{7.0.1}$$

We next apply the results of §6.

Lemma 7.1. *In the ring R, define the element $u = -z_1 z_2 z_3^{-2}$ and the subset*

$$S = \{z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}, -(z_1/z_3)^{\pm 1}, -(z_2/z_3)^{\pm 1}, (z_1 z_2/z_3)^{\pm 1}\}.$$

Then for any $\eta_1, \eta_2, \eta_3 \in \mu$ with $g(\eta_1, \eta_2, \eta_3) = 0$, there exists an element $h \in R$ with $h(\eta_1, \eta_2, \eta_3) = 0$ of one of the following forms:

(a) *$h = \eta \pm 1$ for some $\eta \in S \cup \{u, u^{-1}\}$; or*
(b) *$h = u + u^{-1} + \sum_{\eta \in T} \eta$ for some subset T of S with $\#T \leq 6$ which is invariant under the substition $z_i \mapsto z_i^{-1}$.*

Proof. We apply Theorem 6.1 to the cyclotomic relation of weight 16 obtained from g by separating into monomials with coefficients ± 1, taking u and u^{-1} twice each, then evaluating at $z_i = \eta_i$. If any of the 16 terms is equal to its own conjugate, then (a) holds; we may thus assume that this does not occur.

By Theorem 6.1, this cyclotomic relation admits a partition into indecomposable cyclotomic relations; by Lemma 6.7, this partition can further be taken to be stable under complex conjugation. If we group together conjugate pairs, the two evaluations of u must end up in separate parts; hence one of these parts has weight at most 8, and so (b) holds. □

We finally proceed to solve the desired equation.

Lemma 7.2. *If $\eta_1, \eta_2, \eta_3 \in \mu$ satisfy $g(\eta_1, \eta_2, \eta_3) = 0$, then either there exists $\zeta \in \mu$ with*

$$\eta_1 = \eta_2 = \zeta, \eta_3 = 1 \quad \text{or} \quad \eta_1 = \eta_2 = \zeta, \eta_3 = -\zeta, \tag{7.2.1}$$

or $\eta_1, \eta_2, \eta_3 \in \mathbb{Q}(\mu_N)$ for $N \in \{15, 21, 24\}$; more precisely the orders of η_1, η_2, η_3 must fit one of the patterns listed in Table 2.

Order of η_1	Order of η_2	Orders of η_3
1	2	8
1	4	24
2	2	4
2	4	6,12
3	30	10, 15, 30
4	4	3, 12
6	7	21
7	7	7, 14
30	30	5, 6, 10, 15, 30

TABLE 2. Orders of elements of sporadic solutions in Lemma 7.2.

Proof. Consider the elements $h \in R$ of the forms given by Lemma 7.1 as the vertices of a Cayley graph for the action of the group G and the generators specified above, also adding an edge from h to $g - h$ when both occur as vertices. Using SageMath, we compute a set U of representatives of the connected components of this graph; we have $\#U = 16$. By Lemma 7.1, our original triple (η_1, η_2, η_3) is G-equivalent to one which is a zero of some $h \in U$.

For each $h \in U$, we compute the *torsion closure* of the ideal (g, h) of R in the sense of [9, §7], i.e., the maximal ideal of R whose support contains every solution to $g(\eta_1, \eta_2, \eta_3) = h(\eta_1, \eta_2, \eta_3) = 0$ with $\eta_1, \eta_2, \eta_3 \in \mu$. This computation in SageMath (for all h) takes under 5 minutes on a laptop, using the algorithm described in [9, §7] as implemented in [10].

Of the associated primes of the resulting torsion closures, two are the one-dimensional ideals corresponding to the parametric solutions (7.2.1). The rest are zero-dimensional ideals corresponding to Galois orbits of sporadic solutions in $\mathbb{Q}(\mu_N)$ for $N \in \{15, 21, 24\}$; we construct Table 2 by direct inspection. □

Remark 7.3. We sketch an alternate proof of Lemma 7.2 that can in principle be carried out by hand, although we do not do this completely here.

Suppose first that $h \in U$ arises from case (a) of Lemma 7.1. Modulo the ideal $(h, 2)$ of R, we may write g as indicated, and then deduce the indicated consequences from Remark 6.9. (The listed values of h cover all G-orbits.)

h	g modulo $(h,2)$	Consequence
$z_1 \pm 1$	$z_2 + z_2^{-1}$	$\eta_2^4 = 1$
$z_1 z_2 z_3^{-1} \pm 1$	$z_3 + z_3^{-1}$	$\eta_3^4 = 1$
$z_1 z_2 z_3^{-2} \pm 1$	$z_1^{-2}(z_1 + z_2)(z_1 + z_2^{-1})$	$\eta_1^4 = \eta_2^{\pm 4}$

Similarly, if h arises from case (b) with $T = \emptyset$, then $\eta_1 \eta_2 \eta_3^{-2} = \pm i$ and $g \equiv z_1^{-2}(z_1 + z_2)(z_1 + z_2^{-1}) \pmod{h, 1+i}$, so by Remark 6.9 we have $\eta_1^8 = \eta_2^{\pm 8}$. With further calculation, this yields the parametric solutions (7.2.1) plus solutions with $\eta_1, \eta_2, \eta_3 \in \mathbb{Q}(\mu_N)$ for $N = 24$.

Suppose next that $h \in U$ arises from case (b) of Lemma 7.1. We have already treated the case $\#T = 0$. If $\#T = 2$, then $T = \{\mu, \mu^{-1}\}$ for some $\mu \in S$; the cases $\mu = z_2, -z_2 z_3^{-1}$ cover all G-orbits. Since Table 1 contains no entries with $n = 4$, either $u + \mu$ or $u + \mu^{-1}$ evaluates to 0. With further calculation, this yields the parametric solutions (7.2.1) plus solutions with $\eta_1, \eta_2, \eta_3 \in \mathbb{Q}(\mu_N)$ for $N \in \{7, 12, 15\}$.

If $\#T = 4$, then up to G-action we may take T to be one of four options. One of these is

$$T = \{(-z_1 z_3^{-1})^{\pm 1}, (-z_2 z_3^{-1})^{\pm 1}\},$$

in which we have the algebraic relation $(-z_1 z_3^{-1})(-z_2 z_3^{-1}) = -u$. In this case, we first solve the equation $h(\eta_1, \eta_2, \eta_3) = 0$ in roots of unity; this yields solutions with $\eta_1 \eta_3^{-1}, \eta_2 \eta_3^{-1} \in \mathbb{Q}(\mu_N)$ with $N = 24$. We then substitute into g and solve further to confirm that $\eta_1, \eta_2, \eta_3 \in \mathbb{Q}(\mu_N)$.

The remaining options for T with $\#T = 4$ are

$$\{z_1^{\pm 1}, z_2^{\pm 1}\}, \{z_2^{\pm 1}, (-z_2 z_3^{-1})^{\pm 1}\}, \{z_3^{\pm 1}, (-z_2 z_3^{-1})^{\pm 1}\}.$$

By Lemma 6.7, either h corresponds to the unique sequence listed in Table 1 with $n = 6$ rotated by ± 1, or h splits into two conjugate relations of type R_3. In the first case, we must have $\eta_1, \eta_2, \eta_3 \in \mathbb{Q}(\mu_N)$ for $N = 15$ without further calculation. (When $T = \{z_1^{\pm 1}, z_2^{\pm 1}\}$ solving for η_3 requires a square root, but ends up not forcing an increase in N.) In the second case, u equals a cube root of unity times one of $z_2^{\pm 1}, (-z_2 z_3^{-1})^{\pm 1}$; with further calculation, this yields solutions with $\eta_1, \eta_2, \eta_3 \in \mathbb{Q}(\mu_N)$ for $N \in \{15, 24\}$.

If $\#T = 6$, then both h and $g - h$ correspond to sequences listed in Table 1 rotated by ± 1. (Note that h cannot be the sum of two disjoint conjugate minimal sequences because Table 1 contains no entries with $n = 4$.) In particular, since z_1, z_2, z_3 each appear in either h or $g - h$, we must have $\eta_1, \eta_2, \eta_3 \in \mathbb{Q}(\mu_N)$ for $N \in \{15, 21\}$ without further calculation.

8. Geometric decompositions

With Lemma 7.2 in hand, we now proceed to the proof of Theorem 1.1 and Corollary 1.2.

Proof of Theorem 1.1. As noted earlier, the LMFDB asserts this result in all cases where $\dim(A) \leq 6$, so we may ignore those cases in what follows. Since the cases $n = 1, 2, 7, 30$ are excluded by our dimension bound, Theorem 4.1 implies that the real Weil polynomial associated to A equals $P_n(3 - x)$.

Suppose that α_1, α_2 are distinct Frobenius eigenvalues of A such that $\eta_3 = \alpha_1/\alpha_2$ is a root of unity. By Lemma 5.2, the roots of unity η_1, η_2 of order n corresponding to α_1, α_2 via (5.1.1) satisfy $g(\eta_1, \eta_2, \eta_3) = 0$. Note that each of the exceptional

cases listed in Table 2 includes a now-excluded value of n, and that the first family listed in (7.2.1) is inconsistent with the hypothesis that $\alpha_1 \neq \alpha_2$. Consequently, Lemma 7.2 implies that η_1, η_2, η_3 must belong to the second family listed in (7.2.1); that is, α_1 and α_2 are the two roots of (5.1.1) for some common value of η.

From the previous calculation, it follows that for any positive integer m, the Weil polynomial associated to $A_{\mathbb{F}_{2^m}}$ is either irreducible or the square of an irreducible Weil polynomial. Moreover, the latter outcome occurs when $m = n$: for each root of unity η of order n, both roots of (5.1.1) occur as Frobenius eigenvalues of A_n and their ratio is $-\eta$. We deduce that the Weil polynomial associated to $A_{\mathbb{F}_{q^n}}$ is the square of an irreducible Weil polynomial $Q(x)$, and moreover no two of the roots of $Q(x)$ have ratio equal to a nontrivial root of unity.

If n is not a power of 2, then A is ordinary by Lemma 4.3, as then is $A_{\mathbb{F}_{q^n}}$. Hence Corollary 3.3 implies that $Q(x)$ is the Weil polynomial associated to an abelian variety over $\mathbb{F}_{q^n}$, so we may apply Lemma 2.1 to deduce that $A_{\overline{\mathbb{F}}_q}$ is isogenous to the square of an abelian variety.

If n is a power of 2, then we may use our dimension bound to reduce to the case $n \geq 8$. Lemma 4.3 implies that the slopes of the Newton polygon of A are all equal to $2/n$ or $1 - 2/n$; we may thus apply Lemma 2.2 to deduce that A is geometrically simple. □

Proof of Corollary 1.2. By Theorem 4.1, there exists a unique integer n_i such that B_i is an isogeny factor of A_{n_i}. Let α_i be a Frobenius eigenvalue of B_i. By Theorem 3.1, $\mathrm{Hom}(B_{1,\overline{\mathbb{F}}_q}, B_{2,\overline{\mathbb{F}}_q}) \neq 0$ if and only if some conjugate of α_2 equals α_1 times a root of unity. Using this criterion, it is straightforward to verify the "if" implication.

To check the "only if" implication, we may assume that B_1 and B_2 are not isogenous and that α_1/α_2 is a root of unity. If $n_1 = n_2$, then by Theorem 4.1 the common value is in $\{7, 30\}$. If $n_1 \neq n_2$, we may choose a root of unity η_i of order n_i associated to α_i via Lemma 5.1; by Lemma 7.2, n_1 and n_2 must appear as the first two entries in some row of Table 2. □

9. Additional properties

In [2], it is shown for any fixed q, any sufficiently large positive integer is the order of some abelian variety over $\mathbb{F}_q$ which is simultaneously ordinary, geometrically simple, and principally polarizable. It is thus natural to ask how these conditions interact for simple abelian varieties of order 1 over $\mathbb{F}_2$.

We first consider the combination of the ordinary and geometrically simple conditions. From the proof of Theorem 1.1 and our calculation of Newton polygons (Lemma 4.3), we obtain the following.

Corollary 9.1. *Let A be a simple abelian variety over $\mathbb{F}_2$ of order 1. Then A cannot be both ordinary and geometrically simple. In addition, if $\dim(A) \geq 3$, then A is either ordinary or geometrically simple (but not both).*

As for the principally polarizable condition, we have the following partial result.

Theorem 9.2. *Let n be a power of an odd prime p. Then A_n is isogenous to a principally polarizable abelian variety.*

Proof. Let α be a Frobenius eigenvalue of A_n and choose $\eta \in \mu$ of order n for which (5.1.1) holds; then $\eta \in \mathbb{Q}(\alpha)$. Define

$$\beta = \alpha + 2\alpha^{-1}, \qquad \xi = \eta + \eta^{-1};$$

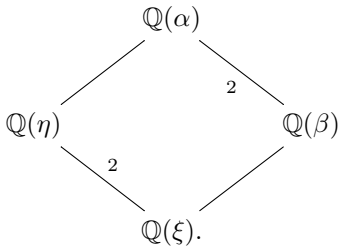
we derive from (5.1.1) the equation

$$\beta^2 + (\xi - 2)\beta - (2 + 3\xi) = 0,$$

which as a quadratic equation in β has discriminant

$$(\xi - 2)^2 + 4(2 + 3\xi) = (\xi + 2)(\xi + 6).$$

We now have the following field diagram:



Let v be a prime of $\mathbb{Q}(\xi)$ lying above p; then modulo v, ξ is congruent to 2 and so $(\xi + 2)(\xi + 6)$ is congruent to 32. As a result, v does not ramify in $\mathbb{Q}(\beta)$; since v does ramify in $\mathbb{Q}(\eta)$, every prime of $\mathbb{Q}(\beta)$ above v ramifies in $\mathbb{Q}(\alpha)$. We may thus apply [7, Theorem 1.1] to deduce that A_n is isogenous to a principally polarizable abelian variety. □

Remark 9.3. For positive integers n such that the simple isogeny factors of A_n are of dimension at most 6, LMFDB reports the following as to whether or not these factors are isogenous to a principally polarizable abelian variety.

- Yes: $n = 1, 2, 3, 4, 5, 7, 9$.
- No: $n = 6, 10, 12, 14, 18, 30$.
- Unknown: $n = 8$.

It may be possible to collect more data using the methods of [14] and [1], especially when A_n is ordinary (which by Lemma 4.3 occurs when n is not a power of 2).

References

[1] J. Bergström, V. Karemaker, and S. Marseglia, Polarizations of abelian varieties over finite fields via canonical liftings, arXiv:2101.05531v3 (2021).
[2] R. van Bommel, E. Costa, W. Li, B. Poonen, and A. Smith, Abelian varieties of prescribed order over finite fields, arXiv:2106.13651v1 (2021).
[3] L. Christie, K.J. Dykema, and I. Klep, Classifying minimal vanishing sums of roots of unity, arXiv:2008.11268v1 (2020).
[4] J.H. Conway and A.J. Jones, Trigonometric Diophantine equations (On vanishing sums of roots of unity), *Acta Arith.* **30** (1976), 229–240.
[5] T. D'Nelly-Warady and K.S. Kedlaya, GitHub repository `https://github.com/mwarady22/Geometric-decomposition-of-abelian-varieties-of-order-1`.
[6] T. Dupuy, K.S. Kedlaya, D. Roe, and C. Vincent, Isogeny classes of abelian varieties over finite fields in the LMFDB, in *Arithmetic Geometry, Number Theory, and Computation*, Simons Symposia, Springer, 2022, 375–448.
[7] E.W. Howe, Kernels of polarizations of abelian varieties over finite fields, *J. Algebraic Geom.* **5** (1996), 583–608.

[8] G.J. Janusz, *Algebraic Number Fields*, second edition, Graduate Studies in Math. 7, Amer. Math. Soc., Providence, 1996.
[9] K.S. Kedlaya, A. Kolpakov, B. Poonen, and M. Rubinstein, Space vectors forming rational angles, arXiv:2011.14232v1 (2020).
[10] K.S. Kedlaya, A. Kolpakov, B. Poonen, and M. Rubinstein, GitHub repository `https://github.com/kedlaya/tetrahedra/`.
[11] The LMFDB Collaboration, L-Functions and Modular Forms Database, `https://lmfdb.org` (retrieved July 2022).
[12] M.L. Madan and S. Pal, Abelian varieties and a conjecture of R. M. Robinson, *J. reine angew. Math.* **291** (1977), 78–91.
[13] Yu.I. Manin, The theory of commutative formal groups over fields of finite characteristic [Russian], *Usp. Math.* **18** (1963), 3–90; English translation, *Russ. Math. Surveys* **18** (1963), 1–80.
[14] S. Marseglia, Computing square-free polarized abelian varieties over finite fields, *Math. Comp.* **90** (2021), 953–971.
[15] B. Poonen and M. Rubinstein, The number of intersection points made by the diagonals of a regular polygon, *SIAM J. Discrete Math.* **11** (1998), 135–156.
[16] R.M. Robinson, Conjugate algebraic units in a special interval, *Math. Z.* **154** (1977), 31–40.
[17] The Sage Developers, SageMath version 9.6, 2022, `https://www.sagemath.org`.
[18] W.C. Waterhouse and J.S. Milne, Abelian varieties over finite fields, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), pp. 53–64. Amer. Math. Soc., Providence, R.I., 1971.
[19] Ł. Włodarski, On the equation $\cos\alpha_1+\cos\alpha_2+\cos\alpha_3+\cos\alpha_4 = 0$, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **12** (1969), 147–155.