*Bull. London Math. Soc.* 46 (2014) 779–792 
doi:10.1112/blms/bdu033

# Abelian surfaces over finite fields with prescribed groups

Chantal David, Derek Garton, Zachary Scherr, Arul Shankar,
Ethan Smith and Lola Thompson

Abstract

Let $A$ be an abelian surface over $\mathbb{F}_q$, the field of $q$ elements. The rational points on $A/\mathbb{F}_q$ form an abelian group $A(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}$. We are interested in knowing which groups of this shape actually arise as the group of points on some abelian surface over some finite field. For a fixed prime power $q$, a characterization of the abelian groups that occur was recently found by Rybakov. One can use this characterization to obtain a set of congruences on certain combinations of coefficients of the corresponding Weil polynomials. We use Rybakov's criterion to show that groups $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}$ do not occur if $n_1$ is very large with respect to $n_2, n_3, n_4$ (Theorem 1.1), and occur with density zero in a wider range of the variables (Theorem 1.2).

## 1. *Introduction*

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_p$. It is well known that the points on $E$ over $\mathbb{F}_p$ form a finite abelian group $E(\mathbb{F}_p)$ having at most two invariant factors, that is,

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z}, \tag{1.1}$$

for some positive integers $n_1, n_2$. It is natural to ask which groups arise in this manner as $p$ runs through all primes and as $E$ runs through all curves over $\mathbb{F}_p$. Let $S(N_1, N_2)$ be the set of pairs of integers $n_1 \leqslant N_1, n_2 \leqslant N_2$ such that there exist a prime $p$ and a curve $E/\mathbb{F}_p$ for which (1.1) holds. The problem of estimating the size of $S(N_1, N_2)$ was first considered by Banks, Pappalardi, and Shparlinski [**1**], who gave precise conjectures and numerical evidence for this problem. In particular, they conjectured that the 'very split' groups (when $n_1$ is very large compared to $n_2$) occur with density zero. This was proven by Chandee, David, Koukoulopoulos, and Smith [**2**], who showed that

$$\#S(N_1, N_2) = \underline{o}(N_1N_2),$$

when $N_1 \geqslant \exp(N_2^{1/2+\varepsilon})$, or equivalently, when $N_2 \leqslant (\log N_1)^{2-\varepsilon}$. Positive density results were also conjectured in [**1**] and proved in part in [**2**].

In this paper, we examine analogous questions for abelian surfaces over finite fields. Here and throughout, $q$ will denote the prime power $p^r$, and $A$ will denote an abelian surface over the finite field $\mathbb{F}_q$. The points on $A$ over $\mathbb{F}_q$ possess the structure of a finite abelian group $A(\mathbb{F}_q)$ having at most four invariant factors, that is,

$$A(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}, \tag{1.2}$$

for some positive integers $n_1, n_2, n_3, n_4$. For the sake of convenience, we will use the notation $G(n_1, n_2, n_3, n_4)$ to refer to the group on the right-hand side of (1.2). We then want to study

Received 2 July 2013; revised 2 March 2014; published online 19 June 2014.

2010 *Mathematics Subject Classification* 11G10 (primary), 11K06 (secondary).

Arul Shankar was partially supported by NSF grant DMS-1128155.

which of the groups $G(n_1, n_2, n_3, n_4)$ actually occur when we vary over all finite fields $\mathbb{F}_q$ and over all abelian surfaces $A/\mathbb{F}_q$.

For fixed $q$, a characterization of the groups occurring as the group of points on a general abelian variety was recently found by Rybakov [**10**, **11**]. Rybakov's elegant criterion relates the Newton polygon of the characteristic polynomial of the variety to the Hodge polygon of the group. The work of Rybakov may be viewed as generalizing Rück's characterization for elliptic curves [**8**] to abelian varieties of any dimension. We give a detailed description of these results in Section 2.

As with the case of elliptic curves, we expect that the 'very split' groups $G(n_1, n_2, n_3, n_4)$ (namely, when $n_1, n_2$ are large with respect to $n_3, n_4$) are less likely to occur. Rybakov's criterion, for example, shows that whenever there is an abelian variety with $N$ points over $\mathbb{F}_q$, the cyclic group of order $N$ will always occur. This is compatible with the general philosophy of the Cohen–Lenstra heuristics, which predict that random abelian groups naturally occur with probability inversely proportional to the size of their automorphism groups. Note that the very split groups have many more automorphisms than the cyclic group of the same size. We refer the reader to [**3**] or [**6**, Theorem 1.2.10] for an exact count.

We now state our main results. We recall that an abelian variety defined over a field $K$ is simple if it is not $K$-isogenous to a product of abelian varieties of lower dimension. Our first result is that some groups never occur for simple abelian surfaces over $\mathbb{F}_q$. In particular, when $n_1$ is too large with respect to $n_2, n_3, n_4$, the group $G(n_1, n_2, n_3, n_4)$ does not arise as the group of points on any simple abelian variety over any finite field.

THEOREM 1.1. *Suppose that $n_1, n_2, n_3, n_4$ are positive integers. If*

$$n_1 \geqslant 60 n_2^{1/4} n_3^{3/2} n_4^{3/4} + 1,$$

*then for every $q$, there is no simple abelian surface $A/\mathbb{F}_q$ with $A(\mathbb{F}_q) \simeq G(n_1, n_2, n_3, n_4)$.*

This is very different from the case of elliptic curves where one cannot rule out the possibility of occurrence for the group $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1 n_2\mathbb{Z}$ merely based on the relative sizes of $n_1$ and $n_2$. For instance, while the group $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}$ is very unlikely to occur as the group of points for some elliptic curve [**2**], and while examples of such groups are known not to occur at all [**1**], it is quite likely that there are infinitely many examples of such groups that arise in this way. In particular, this would follow from the standard conjecture that there are infinitely many primes of the form $n_1^2 + 1$.

We also show that fewer groups occur in a probabilistic sense. Our next result essentially says that if $n_1$ or $n_2$ is very large compared to $n_3$ and $n_4$, then $G(n_1, n_2, n_3, n_4)$ occurs with probability zero. Given $N_1, N_2, N_3, N_4 \geqslant 1$, we define $S(N_1, N_2, N_3, N_4)$ to be the set of quadruples $(n_1, n_2, n_3, n_4)$ for which $N_j \leqslant n_j \leqslant 2N_j$ for $1 \leqslant j \leqslant 4$ and there exist a prime power $q$ and a simple abelian surface $A/\mathbb{F}_q$ with $A(\mathbb{F}_q) \simeq G(n_1, n_2, n_3, n_4)$. Throughout, we write $f = \underline{o}(g)$ as $x \to \infty$ if $f/g \to 0$ as $x \to \infty$.

THEOREM 1.2. *If*

$$\frac{N_1 N_2^{1/4}}{N_3^{1/2} N_4^{1/4}} \to \infty,$$

*as $N_2 N_4 \to \infty$, then*

$$\# S(N_1, N_2, N_3, N_4) = \underline{o}(N_1 N_2 N_3 N_4),$$

*as $N_2 N_4 \to \infty$.*

REMARK 1.3. Just as this work was accepted for publication, Pierre Le Boudec shared with us a proof that $G(n_1, n_2, n_3, n_4)$ does not occur at all for $n_1 n_2^{1/4}/n_3^{1/2} n_4^{1/4}$ large enough. In particular, this means that the conclusion of Theorem 1.1 can be strengthened to $\#S(N_1, N_2, N_3, N_4) = 0$. Unfortunately, it is not quite as easy as with the elliptic curve case to say what one ought to expect for the distribution of groups in this setting. This is due to the fact that the criteria for existence (see Theorems 2.3 and 2.4) are more complicated in higher dimensions. In fact, neither our proofs nor the proof that Le Boudec shared with us seem to use the full strength of Rybakov's criteria.

## 2. *Weil polynomials and groups of abelian surfaces*

A classification of simple abelian varieties over $\mathbb{F}_q$ (up to $\mathbb{F}_q$-isogeny) is given by Tate–Honda theory, which gives a one-to-one correspondence between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes of Weil numbers (algebraic integers whose conjugates have absolute value $q^{1/2}$). This classification can be stated using the characteristic polynomial of the Frobenius endomorphism $\pi_A$ of $A/\mathbb{F}_q$. This polynomial, which we denote by $f_A(T)$, determines $A$ up to isogeny, and it has Weil numbers as its roots. For an abelian surface $A/\mathbb{F}_q$, we write

$$f_A(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 q T + q^2.$$

The number of $\mathbb{F}_q$-rational points on $A$ is equal to $f_A(1)$ and hence is an invariant of the isogeny class. The fact that the roots of $f_A(T)$ are Weil numbers implies that

$$(\sqrt{q} - 1)^4 \leqslant \#A(\mathbb{F}_q) \leqslant (\sqrt{q} + 1)^4. \tag{2.1}$$

If $A$ is a simple abelian surface, then $f_A(T) = h_A(T)^e$ where $h_A(T)$ is an irreducible polynomial in $\mathbb{Z}[T]$ whose roots are Weil numbers. Furthermore, the endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field if and only if $e = 1$. Computing the local invariants of the algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ allows one to obtain a correspondence between the set of simple abelian surfaces over $\mathbb{F}_q$ such that $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field and the set of irreducible polynomials $f(T)$ of degree 4 whose roots are Weil numbers and whose monic irreducible divisors $f_i(T)$ over $\mathbb{Q}_p$ have integer values of $\nu_p(f_i(0))/\nu_p(q)$. Here and throughout, we use the notation $\nu_p$ to denote the usual $p$-adic valuation. Rück [**9**] gave the following explicit characterization of these polynomials.

THEOREM 2.1 (Rück). *The set of $f_A(T)$ for all abelian varieties $A$ over $\mathbb{F}_q$ of dimension 2 whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field is equal to the set of polynomials $f(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 q T + q^2$ where the integers $a_1$ and $a_2$ satisfy the conditions*

- (a) $|a_1| < 4q^{1/2}$, $2|a_1|q^{1/2} - 2q < a_2 < a_1^2/4 + 2q$;
- (b) $a_1^2 - 4a_2 + 8q$ *is not a square in* $\mathbb{Z}$; *and*
- (c) *either*
  - (i) $\nu_p(a_1) = 0, \nu_p(a_2) \geqslant r/2$ *and* $(a_2 + 2q)^2 - 4qa_1^2$ *is not a square in* $\mathbb{Z}_p$;
  - (ii) $\nu_p(a_2) = 0$; *or*
  - (iii) $\nu_p(a_1) \geqslant r/2$, $\nu_p(a_2) \geqslant r$, *and* $f(T)$ *has no root in* $\mathbb{Z}_p$.

The polynomials $f_A(T)$ corresponding to simple abelian surfaces $A$ over $\mathbb{F}_q$ whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is not a field are much rarer. They can be described explicitly as well, see [**13**, Theorem 4.1] and [**14**, Lemma 1].

Theorem 2.2 (Waterhouse and Xing). *The characteristic polynomial $f_A(T)$ of any simple abelian variety $A$ of dimension 2 over $\mathbb{F}_q$ whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is not field must be of the form*

(a) $f_A(T) = (T^2 - q)^2$ *and $r$ is odd;*
(b) $f_A(T) = (T^2 + q)^2$, *$r$ is even, and $p \equiv 1 \pmod 4$; or*
(c) $f_A(T) = (T^2 \pm q^{1/2}T + q)^2$, *$r$ is even, and $p \equiv 1 \pmod 3$.*

The group structures for these 'exceptional' polynomials $f_A(T)$ were studied by Xing [**14**, **15**]. In the respective cases (corresponding to Theorem 2.2), Xing showed that the group structures which arise are precisely

(a) $(\mathbb{Z}/(q-1)\mathbb{Z})^2$, $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/((q-1)/2)\mathbb{Z})^2$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/((q-1)/2)\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z}$;
(b) $(\mathbb{Z}/(q+1)\mathbb{Z})^2$; or
(c) $(\mathbb{Z}/(q \pm q^{1/2} + 1)\mathbb{Z})^2$.

We refer the reader to [**14**] for a precise description of when each group corresponding to the first case arises. Thus, the abelian surfaces $A$ whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is not a field give rise to very few groups $G(n_1, n_2, n_3, n_4)$. More importantly, $n_1, n_2 \leqslant 2$ for all such groups, and hence they do not satisfy the conditions of Theorem 1.1 or Theorem 1.2. Therefore, we exclude this case from consideration for the remainder of the paper.

For the typical case of abelian surfaces whose algebra is a field, there is a very elegant criterion due to Rybakov [**10**, **11**] that characterizes those isogeny classes which contain a variety $A$ with $A(\mathbb{F}_q) \simeq G(n_1, n_2, n_3, n_4)$. The result of Rybakov applies to abelian varieties of any dimension $g \geqslant 1$. We state it below in full generality and then for the particular case of abelian surfaces. We first need some definitions.

Let $\ell$ be a prime, and let $Q(T) = \sum_i Q_i T^i$ be a polynomial of degree $d$ with $Q(0) = Q_0 \neq 0$. The *Newton polygon* $\mathrm{Np}_\ell(Q)$ is the boundary (without vertical lines) of the lower convex hull of the points $(i, \nu_\ell(Q_i))$ for $0 \leqslant i \leqslant d$ in $\mathbb{R}^2$. Now let $0 \leqslant m_1 \leqslant m_2 \leqslant \ldots \leqslant m_r$ be nonnegative integers, and let $H = \bigoplus_{i=1}^r \mathbb{Z}/\ell^{m_i}\mathbb{Z}$. The *Hodge polygon* $\mathrm{Hp}_\ell(H, r)$ is the convex polygon with vertices $(i, \sum_{j=1}^{r-i} m_j)$ for $0 \leqslant i < r$. Given an abelian group $G$, we let $G_\ell$ denote the $\ell$-primary component of $G$. The following is the main result of [**10**].

Theorem 2.3 (Rybakov). *Let $A$ be an abelian variety of dimension $g$ over a finite field whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field. Let $f_A(T)$ denote its characteristic polynomial, and let $G$ be an abelian group of order $f_A(1)$ that can be generated by $2g$ or fewer elements. Then $G$ is the group of points on some variety in the isogeny class of $A$ if and only if $\mathrm{Np}_\ell(f_A(1-T))$ lies on or above $\mathrm{Hp}_\ell(G_\ell, 2g)$ for every prime number $\ell$.*

The preceding theorem is the original formulation of [**10**], but it is easy to restate the theorem without any reference to the Newton polygon or the Hodge polygon. Namely, we can state the theorem in terms of the divisibility of the derivatives of $f_A(T)$ at $T = 1$. We present this version below.

Theorem 2.4 (Rybakov). *Let $A$ be an abelian variety of dimension $g$ over a finite field whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field. Let $f_A(T)$ denote its characteristic polynomial, and let*

$$G = \mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_{2g}\mathbb{Z} \quad \text{where } N_1 \mid N_2 \mid \ldots \mid N_{2g},$$

*and such that $\#G = N_1 \dots N_{2g} = f_A(1)$. Then $G$ is the group of points on some variety in the isogeny class of $A$ if and only if*

$$\prod_{j=1}^{2g-k} N_i \text{ divides } \frac{f_A^{(k)}(1)}{k!} \quad \text{for } k = 0, \dots, 2g-1.$$

*Proof.* We first write the Taylor expansion

$$f_A(1-T) = \sum_{k=0}^{2g} \frac{f_A^{(k)}(1)}{k!}(-T)^k.$$

For each prime $\ell$, the condition that $\mathrm{Np}_\ell(f_A(1-T))$ lies on or above $\mathrm{Hp}_\ell(G_\ell, 2g)$ means that

$$\nu_\ell\left(\prod_{j=1}^{2g-k} N_j\right) \leqslant \nu_\ell\left(\frac{f_A^{(k)}(1)}{k!}\right) \quad \text{for } k = 0, \dots, 2g-1.$$

By putting all of the primes together, we see that

$$\prod_{j=1}^{2g-k} N_j \text{ divides } \frac{f_A^{(k)}(1)}{k!} \quad \text{for } k = 0, \dots, 2g-1.$$

□

Recall that we always use the notation

$$G(n_1, n_2, n_3, n_4) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z},$$

for positive integers $n_1, n_2, n_3, n_4$ to describe the group of points on an abelian variety. In particular, $\#G(n_1, n_2, n_3, n_4) = n_1^4 n_2^3 n_3^2 n_4$. Thus, for the case of abelian surfaces, we can rewrite the conditions of Theorem 2.4 as follows.

Corollary 2.5. *Let $A/\mathbb{F}_q$ be an abelian surface, and suppose that $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field. Let $f_A(T) = T^4 + a_1T^3 + a_2T^2 + a_1qT + q^2$ denote its Weil polynomial. Then the isogeny class of $A$ contains a variety with group of points isomorphic to $G(n_1, n_2, n_3, n_4)$ if and only if*

$$n_1^4 n_2^3 n_3^2 n_4 = f_A(1) = q^2 + a_1q + a_2 + a_1 + 1 \tag{2.2}$$

*and*

$$4 + 3a_1 + 2a_2 + qa_1 \equiv 0 \pmod{n_1^3 n_2^2 n_3}, \tag{2.3}$$
$$6 + 3a_1 + a_2 \equiv 0 \pmod{n_1^2 n_2}, \tag{2.4}$$
$$4 + a_1 \equiv 0 \pmod{n_1}. \tag{2.5}$$

We remark that Corollary 2.5 implies that if $f_A(1) = N$, then the cyclic group of order $N$ occurs as a group of points on some abelian surface in the isogeny class of $A$ since in that case we have $n_1 = n_2 = n_3 = 1$, so the congruences (2.3)–(2.5) are trivially satisfied.

## 3. *Key proposition*

In this section, we prove the following key proposition. As is somewhat common, for any real number $x$, we write $||x||$ for the distance between $x$ and its nearest integer neighbor. To ease notation, we define

$$\delta = \delta(n_1, n_2, n_3, n_4) = \begin{cases} 1 & \text{if } 2n_3\sqrt{n_2 n_4} \in \mathbb{Z}, \\ \|2n_3\sqrt{n_2 n_4}\| & \text{otherwise,} \end{cases} \tag{3.1}$$

for any positive integers $n_1, n_2, n_3, n_4$.

PROPOSITION 3.1. *Suppose that $A/\mathbb{F}_q$ is an abelian surface and that $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field. Suppose further that $A(\mathbb{F}_q) \simeq G(n_1, n_2, n_3, n_4)$. Then*

$$n_1 < \frac{10 n_3^{1/2} n_4^{1/4}}{\delta n_2^{1/4}} + \frac{1}{n_2^{3/4} n_3^{1/2} n_4^{1/4}}.$$

Theorems 1.1 and 1.2 will follow from Proposition 3.1. Theorem 1.1 follows by specifying lower bounds for $\|\sqrt{m}\|$ that are valid for every integer $m$. For the details, see Section 4. Theorem 1.2 follows from the fact that the triple sequence $2n_3\sqrt{n_2 n_4}$ is uniformly distributed modulo 1; we will prove this in Section 5.

First, we use the congruences of Corollary 2.5 to derive a simpler congruence on $a_1$.

LEMMA 3.2. *Suppose that $q$, $a_1$, $a_2$, $n_1$, $n_2$, $n_3$, and $n_4$ satisfy (2.2)–(2.5). Then*

$$a_1 \equiv -2(q+1) \pmod{n_1^2 n_2}.$$

*Proof.* Reducing (2.2) and (2.3) modulo $n_1^3 n_2^2$ yields

$$q^2 + a_1 q + a_2 + a_1 + 1 \equiv 0 \pmod{n_1^3 n_2^2}, \tag{3.2}$$

$$4 + 3a_1 + 2a_2 + q a_1 \equiv 0 \pmod{n_1^3 n_2^2}. \tag{3.3}$$

Reducing the above congruences modulo $n_1^2 n_2$ and taking their difference gives

$$2a_1 + a_2 + 3 - q^2 \equiv 0 \pmod{n_1^2 n_2}.$$

Subtracting this from (2.4), we obtain

$$a_1 + 3 + q^2 \equiv 0 \pmod{n_1^2 n_2}. \tag{3.4}$$

The remainder of the proof is devoted to showing that $n_1^2 n_2 \mid (q-1)^2$, which together with (3.4) implies the desired congruence $a_1 \equiv -2(q+1) \pmod{n_1^2 n_2}$.

Taking twice (3.2) and subtracting off (3.3) yields

$$2q^2 + a_1 q - a_1 - 2 \equiv 0 \pmod{n_1^3 n_2^2}. \tag{3.5}$$

From (3.4), we know that there is an integer $k$ such that $a_1 = -3 - q^2 + k n_1^2 n_2$. After some slight rearrangement, plugging this expression for $a_1$ into (3.5) gives

$$k n_1^2 n_2 (q-1) - (q-1)^3 \equiv 0 \pmod{n_1^3 n_2^2}. \tag{3.6}$$

Working prime by prime, we will show that (3.6) implies that $n_1^2 n_2 \mid (q-1)^2$. To this end, let $\ell$ be an arbitrary prime, and suppose that $\nu_\ell(n_1^2 n_2) = r$. Then we want to show that $\nu_\ell((q-1)^2) \geqslant r$. Assume for the sake of contradiction that $\nu_\ell((q-1)^2) < r$. Since $\nu_\ell(k n_1^2 n_2) \geqslant r$, it follows that $\nu_\ell(k n_1^2 n_2 - (q-1)^2) = \nu_\ell((q-1)^2)$, and hence

$$\nu_\ell(k n_1^2 n_2 (q-1) - (q-1)^3) = \nu_\ell(q-1) + \nu_\ell(k n_1^2 n_2 - (q-1)^2) = 3\nu_\ell(q-1) < \frac{3r}{2}.$$

On the other hand, since $n_1^3 n_2^2$ divides $k n_1^2 n_2 (q-1) - (q-1)^3$, it follows that

$$3\nu_\ell(n_1) + 2\nu_\ell(n_2) \leqslant \nu_\ell(k n_1^2 n_2 (q-1) - (q-1)^3) < \frac{3r}{2} = \frac{3}{2}(2\nu_\ell(n_1) + \nu_\ell(n_2)).$$

However, this implies that $\nu_\ell(n_2) < 0$, which is impossible since $n_2$ is an integer. $\square$

LEMMA 3.3. *Suppose that $A/\mathbb{F}_q$ is an abelian surface, $\mathrm{End}_{\mathbb{F}_q}(A)\otimes\mathbb{Q}$ is a field, and $A(\mathbb{F}_q)\simeq G(n_1,n_2,n_3,n_4)$. If $f_A(T)=T^4+a_1T^3+a_2T^2+qa_1T+q^2$ is the characteristic polynomial of $A/\mathbb{F}_q$, then there exists an integer $k$ such that*

$$a_1 = kn_1^2n_2 - 2(q+1)$$

*and*

$$2n_3\sqrt{n_2n_4}\left(\frac{\sqrt{q}-1}{\sqrt{q}+1}\right)^2 < k < 2n_3\sqrt{n_2n_4}\left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right)^2. \tag{3.7}$$

*Proof.* By Theorem 2.1(a), we know that $-4\sqrt{q}<a_1<4\sqrt{q}$. By Lemma 3.2, there exists an integer $k$ such that $a_1=n_1^2n_2k-2(q+1)$. Substituting this into the bounds for $a_1$ and adding $2(q+1)$ to each side of the inequalities yields

$$2q-4\sqrt{q}+2<n_1^2n_2k<2q+4\sqrt{q}+2.$$

Factoring and dividing through by $n_1^2n_2$ allows us to obtain

$$\frac{2(\sqrt{q}-1)^2}{n_1^2n_2}<k<\frac{2(\sqrt{q}+1)^2}{n_1^2n_2}.$$

Since $\#A(\mathbb{F}_q)=n_1^4n_2^3n_3^2n_4$, the Weil bound (2.1) implies that

$$\frac{(\sqrt{q}-1)^2}{n_3\sqrt{n_2n_4}}\leqslant n_1^2n_2\leqslant\frac{(\sqrt{q}+1)^2}{n_3\sqrt{n_2n_4}}.$$

Together these bounds imply (3.7). □

For $q$ large enough, the interval from Lemma 3.3 will contain at most one integer $k$. The following lemma makes this statement precise. Recall the definition of $\delta$ given by (3.1).

LEMMA 3.4. *If $\sqrt{q}\geqslant 10n_3\sqrt{n_2n_4}/\delta$, then the interval (3.7) contains no integral values of $k$ unless $2n_3\sqrt{n_2n_4}$ is an integer, in which case $k=2n_3\sqrt{n_2n_4}$.*

*Proof.* To further ease notation, let $m=2n_3\sqrt{n_2n_4}$. Note that the interval $(m-\delta,m+\delta)$ does not contain an integer unless $m=2n_3\sqrt{n_2n_4}$ is itself an integer, in which case it is the only such integer. Since

$$\left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right)^2=1+\frac{4\sqrt{q}}{(\sqrt{q}-1)^2}\quad\text{and}\quad\left(\frac{\sqrt{q}-1}{\sqrt{q}+1}\right)^2=1-\frac{4\sqrt{q}}{(\sqrt{q}+1)^2},$$

it follows that the interval (3.7) is contained in the interval $(m-\delta,m+\delta)$ if and only if

$$m\frac{4\sqrt{q}}{(\sqrt{q}-1)^2}\leqslant\delta.$$

Factoring the latter inequality and dividing by $\delta$ yields

$$0\leqslant\left(\sqrt{q}-\frac{2m+\delta-2\sqrt{m^2+m\delta}}{\delta}\right)\left(\sqrt{q}-\frac{2m+\delta+2\sqrt{m^2+m\delta}}{\delta}\right). \tag{3.8}$$

Now, since

$$\frac{2m+\delta-2\sqrt{m^2+m\delta}}{\delta}\leqslant 1,$$

it follows that (3.8) holds if and only if

$$\sqrt{q} \geqslant \frac{2m+\delta+2\sqrt{m^2+m\delta}}{\delta}.$$

However,

$$\frac{2m+\delta+2\sqrt{m^2+m\delta}}{\delta} \leqslant \frac{2m+1+2\sqrt{m^2+m+1/4}}{\delta} = \frac{4m+2}{\delta} \leqslant \frac{5m}{\delta},$$

and so (3.8) holds if $\sqrt{q} \geqslant 5m/\delta = 10n_3\sqrt{n_2n_4}/\delta$. □

*Proof of Proposition* 3.1. First, suppose that $k = 2n_3\sqrt{n_2n_4}$ is an integer and

$$a_1 = kn_1^2n_2 - 2(q+1) = 2n_1^2n_2^{3/2}n_3n_4^{1/2} - 2(q+1).$$

Then substitution into (2.2) gives

$$a_2 = n_1^4n_2^3n_3^2n_4 - 1 - \left(2n_1^2n_2^{3/2}n_3n_4^{1/2} - 2(q+1)\right)(q+1) - q^2.$$

Under these assumptions, we then find that

$$a_1^2 - 4a_2 + 8q = 0.$$

According to Theorem 2.1(b), this contradicts the assumption that $\mathrm{End}_{\mathbb{F}_q} \otimes \mathbb{Q}$ is field. Therefore, by Lemmas 3.3 and 3.4, regardless of whether $2n_3\sqrt{n_2n_4}$ is an integer, we see that if $A(\mathbb{F}_q) \simeq G(n_1, n_2, n_3, n_4)$ and $\mathrm{End}_{\mathbb{F}_q} \otimes \mathbb{Q}$ is a field, then $\sqrt{q} < 10n_3\sqrt{n_2n_4}/\delta$. Using this together with the Weil bound (2.1), we have that

$$n_1n_2^{3/4}n_3^{2/4}n_4^{1/4} \leqslant \sqrt{q} + 1 < 10n_3\sqrt{n_2n_4}/\delta + 1.$$

Whence,

$$n_1 < \frac{10n_3^{1/2}n_4^{1/4}}{\delta n_2^{1/4}} + \frac{1}{n_2^{3/4}n_3^{1/2}n_4^{1/4}}.$$ □

## 4. *Proof of Theorem* 1.1

The proof of Theorem 1.1 can be deduced from the following simple observation, which gives a lower bound for $\|2n_3\sqrt{n_2n_4}\|$. As usual, for any real number $x$, we write $[x]$ for the largest integer less than or equal to $x$, and $\{x\} = x - [x]$ for the fractional part of $x$.

LEMMA 4.1. *Let $m$ be an integer that is not a perfect square. Then*

$$\|\sqrt{m}\| > \frac{1}{3\sqrt{m}}.$$

*Proof.* Since $\sqrt{m} = [\sqrt{m}] + \{\sqrt{m}\}$, upon squaring both sides, we find that

$$\begin{aligned} m &= [\sqrt{m}]^2 + 2\{\sqrt{m}\}[\sqrt{m}] + \{\sqrt{m}\}^2 \\ &= [\sqrt{m}]^2 + (\sqrt{m} + [\sqrt{m}])\{\sqrt{m}\} \\ &\leqslant [\sqrt{m}]^2 + 2\sqrt{m}\{\sqrt{m}\}. \end{aligned}$$

Therefore, since $1 < m - [\sqrt{m}]^2$, we have $\{\sqrt{m}\} > 1/2\sqrt{m}$.

Similarly, since we can write $\sqrt{m} = [\sqrt{m}] + 1 - (1 - \{\sqrt{m}\})$, we have that

$$\begin{aligned} m &= ([\sqrt{m}] + 1)^2 - 2(1 - \{\sqrt{m}\})([\sqrt{m}] + 1) + (1 - \{\sqrt{m}\})^2 \\ &= ([\sqrt{m}] + 1)^2 - (\sqrt{m} + [\sqrt{m}] + 1)(1 - \{\sqrt{m}\}) \\ &\geqslant ([\sqrt{m}] + 1)^2 - (2\sqrt{m} + 1)(1 - \{\sqrt{m}\}). \end{aligned}$$

Therefore, since $1 \leqslant ([\sqrt{m}] + 1)^2 - m$, we obtain $1 - \{\sqrt{m}\} \geqslant 1/(2\sqrt{m} + 1) > 1/3\sqrt{m}$. □

*Proof of Theorem* 1.1. In light of Theorem 2.2, we need to consider only abelian surfaces $A$ with $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ a field. In this case, Proposition 3.1 applies, and if there is a prime power $q$ and an abelian surface $A/\mathbb{F}_q$ with group $G(n_1, n_2, n_3, n_4)$, then

$$n_1 < \frac{10 n_3^{1/2} n_4^{1/4}}{\delta n_2^{1/4}} + \frac{1}{n_2^{3/4} n_3^{1/2} n_4^{1/4}} \leqslant \frac{10 n_3^{1/2} n_4^{1/4}}{\delta n_2^{1/4}} + 1,$$

where $\delta$ is as defined by (3.1). By Lemma 4.1,

$$n_1 < 60 n_2^{1/4} n_3^{3/2} n_4^{3/4} + 1,$$

since $\delta \geqslant (6 n_3 \sqrt{n_2 n_4})^{-1}$. □

## 5. *Proof of Theorem* 1.2

In this section, we use the standard notation $f \ll g$ to mean that there exists a positive constant $c$ such that $|f| \leqslant cg$. We also use the notation $n \asymp N$ (in a somewhat nonstandard way) as a shorthand for $N \leqslant n \leqslant 2N$.

To prove Theorem 1.2, we use the fact that for most triples of integers $(n_2, n_3, n_4)$ with $n_j \asymp N_j$ $(2 \leqslant j \leqslant 4)$, the distance between $2n_3\sqrt{n_2 n_4}$ and the nearest integer is larger than any function tending to zero as $N_2 N_4 \to \infty$. This follows from the uniform distribution of $2n_3\sqrt{n_2 n_4}$ modulo one; see Theorem 5.6. For the sake of completeness, we review much of the relevant material here.

Let

$$\mathcal{T}(N_2, N_3, N_4) = \{(n_2, n_3, n_4) : n_2 \asymp N_2, n_3 \asymp N_3, n_4 \asymp N_4\},$$

and let $\{f(n_2, n_3, n_4) : n_2, n_3, n_4 \geqslant 1\}$ be any triply indexed sequence of real numbers. For $0 \leqslant \alpha < \beta \leqslant 1$, let

$$Z_f(N_2, N_3, N_4; \alpha, \beta) = \#\{(n_2, n_3, n_4) \in \mathcal{T}(N_2, N_3, N_4) : \alpha \leqslant \{f(n_2, n_3, n_4)\} \leqslant \beta\},$$

where, as in the previous section, $\{f(n_2, n_3, n_4)\}$ denotes the fractional part of $f(n_2, n_3, n_4)$. We say that the sequence $f(n_2, n_3, n_4)$ is uniformly distributed modulo one if

$$\lim_{N_2, N_3, N_4 \to \infty} \frac{Z_f(N_2, N_3, N_4; \alpha, \beta)}{N_2 N_3 N_4} = \beta - \alpha.$$

By Weyl's criterion, this is equivalent to showing that

$$E_k(N_2, N_3, N_4) := \sum_{\substack{n_2 \asymp N_2, \\ n_3 \asymp N_3, \\ n_4 \asymp N_4}} e(k f(n_2, n_3, n_4)) = \underline{o}(N_2 N_3 N_4),$$

for every integer $k \neq 0$. As usual, we have written $e(x) = e^{2\pi i x}$. We can put this equivalence in quantitative form using the Selberg polynomials. This is explained in [**7**, Chapter 1] for a sequence of one variable. The proof for a sequence of three variables $f(n_2, n_3, n_4)$ follows along the same lines. The next theorem is then the analog of [**7**, Chapter 1, Theorem 1] for triple sequences.

THEOREM 5.1. *Let $f(n_2, n_3, n_4)$ be a sequence of real numbers, and let $0 \leqslant \alpha \leqslant \beta \leqslant 1$. Then*

$$\begin{aligned} &|Z_f(N_2, N_3, N_4; \alpha, \beta) - (\beta-\alpha)\#\mathcal{T}(N_2, N_3, N_4)| \\ &\quad \leqslant \frac{\#\mathcal{T}(N_2, N_3, N_4)}{K+1} + 2\sum_{k=1}^{K}\left(\frac{1}{K+1} + \min\left(\beta-\alpha, \frac{1}{\pi k}\right)\right)|E_k(N_2, N_3, N_4)|, \end{aligned} \tag{5.1}$$

*for any positive integers $N_2, N_3, N_4$, and $K$.*

*Proof.* For each positive integer $K$, let

$$S_K^+(n) = \sum_{-K \leqslant k \leqslant K} \hat{S}_K^+(k) e(kn)$$

be the Selberg polynomial upper bounding the characteristic function of $[\alpha, \beta]$ as defined in [**7**, p. 6]. Then

$$\begin{aligned} Z_f(N_2, N_3, N_4; \alpha, \beta) &\leqslant \sum_{\substack{n_2 \asymp N_2 \\ n_3 \asymp N_3 \\ n_4 \asymp N_4}} S_K^+(f(n_2, n_3, n_4)) \\ &= \sum_{-K \leqslant k \leqslant K} \hat{S}_K^+(k) \sum_{\substack{n_2 \asymp N_2 \\ n_3 \asymp N_3 \\ n_4 \asymp N_4}} e(kf(n_2, n_3, n_4)). \end{aligned}$$

Now, since

$$\hat{S}_K^+(0) = \beta - \alpha + \frac{1}{K+1}$$

and

$$E_0(N_2, N_3, N_4) = \#\mathcal{T}(N_2, N_3, N_4),$$

we have that

$$\begin{aligned} &Z_f(N_2, N_3, N_4; \alpha, \beta) - (\beta-\alpha)\#\mathcal{T}(N_2, N_3, N_4) \\ &\quad \leqslant \frac{\#\mathcal{T}(N_2, N_3, N_4)}{K+1} + \sum_{\substack{-K \leqslant k \leqslant K \\ k \neq 0}} \hat{S}_K^+(k) E_k(N_2, N_3, N_4). \end{aligned}$$

It follows from properties of Selberg polynomials that

$$|\hat{S}_K^+(k)| \leqslant \frac{1}{K+1} + \min\left(\beta - \alpha, \frac{1}{\pi|k|}\right),$$

for $0 < |k| \leqslant K$ (see [**7**, p. 8], for example). Combining the inequalities from above, we have

$$\begin{aligned} &Z_f(N_2, N_3, N_4; \alpha, \beta) - (\beta-\alpha)\,\#\mathcal{T}(N_2, N_3, N_4) \\ &\quad \leqslant \frac{\#\mathcal{T}(N_2, N_3, N_4)}{K+1} + 2\sum_{1 \leqslant k \leqslant K}\left(\frac{1}{K+1} + \min\left(\beta-\alpha, \frac{1}{\pi|k|}\right)\right)|E_k(N_2, N_3, N_4)|. \end{aligned}$$

Using the Selberg polynomials $S_K^-(n)$ as defined in [**7**, p. 6], the other inequality follows, as does the theorem. □

For the remainder of the paper, we will specialize to the sequence $f(n_2, n_3, n_4) = 2n_3\sqrt{n_2 n_4}$. We now bound the sum appearing in Theorem 5.1 to show that the sequence $2n_3\sqrt{n_2 n_4}$ is uniformly distributed modulo 1. In order to obtain our result without any conditions on the relative sizes of the parameters $N_2, N_3, N_4$, we bound the sum appearing in (5.1) in two different ways (Lemmas 5.3 and 5.5). First, we use the following result from [**5**, p. 77].

LEMMA 5.2. *Let $g(t)$ be a real, continuously differentiable function on the interval $[a,b]$, with $|g'(t)| \geqslant \lambda > 0$, and let $N > 0$. Then*

$$\sum_{a\leqslant n\leqslant b} \min\{N, 1/\|g(n)\|\} \ll (|g(b)-g(a)|+1)\left(N + \frac{1}{\lambda}\log(b-a+2)\right).$$

LEMMA 5.3. *For every $\varepsilon > 0$ and $K \geqslant 1$,*

$$\sum_{k\leqslant K} \frac{1}{k}|E_k(N_2,N_3,N_4)| \ll (N_2N_4)^{1/2+\varepsilon}N_3K + (N_2N_4)^{1+\varepsilon}\log 2K.$$

*Proof.* Let

$$b_n = \sum_{n_2\asymp N_2}\sum_{n_4\asymp N_4 n_2n_4=n} 1,$$

and note that $b_n \ll n^{\varepsilon/2}$. Recall the well-known bound

$$\sum_{n\asymp N} e(\alpha n) \ll \min\{N, 1\|\alpha\|\}.$$

See [**4**, p. 199], for example. Applying Lemma 5.2, we have

$$\begin{aligned}\sum_{k\leqslant K}\frac{1}{k}|E_k(N_2,N_3,N_4)| &= \sum_{k\leqslant K}\frac{1}{k}\sum_{N_2N_4\leqslant n\leqslant 4N_2N_4} b_n \sum_{n_3\asymp N_3} e(2kn^{1/2}n_3)\\ &\ll (N_2N_4)^{\varepsilon/2}\sum_{k\leqslant K}\frac{1}{k}\sum_{N_2N_4\leqslant n\leqslant 4N_2N_4}\min\left\{N_3, \frac{1}{\|2kn^{1/2}\|}\right\}\\ &\ll (N_2N_4)^{\varepsilon/2}\sum_{k\leqslant K}(N_2N_4)^{1/2}(N_3 + k^{-1}(N_2N_4)^{1/2}\log(2N_2N_4))\\ &\ll (N_2N_4)^{\varepsilon}((N_2N_4)^{1/2}N_3K + (N_2N_4)\log 2K).\end{aligned}$$

□

We now bound the same sum using the following consequence of the van der Corput method found in [**12**, p. 94].

LEMMA 5.4. *Let $g(t)$ be a twice continuously differentiable function on the interval $[a,b]$ such that $|g''(t)| \asymp \lambda > 0$. Then*

$$\sum_{a\leqslant n\leqslant b} e(g(n)) \ll (b-a+1)\lambda^{1/2} + \lambda^{-1/2}.$$

LEMMA 5.5. *For every $K \geqslant 1$,*

$$\sum_{k\leqslant K}\frac{1}{k}|E_k(N_2,N_3,N_4)| \ll K^{1/2}N_3^{3/2}(N_2N_4)^{3/4} + N_3^{1/2}(N_2N_4)^{3/4}.$$

*Proof.* We first apply Lemma 5.4 with $g(t) = 2kn_3\sqrt{n_2t}$, noting that $|g''(t)| = kn_3\sqrt{n_2}/(2t^{3/2})$. This yields

$$\begin{aligned}\sum_{k\leqslant K}\frac{1}{k}|E_k(N_2,N_3,N_4)| &\ll \sum_{k\leqslant K}\frac{1}{k}\sum_{\substack{n_2\asymp N_2,\\ n_3\asymp N_3}}(N_4^{1/4}(kn_3\sqrt{n_2})^{1/2} + N_4^{3/4}(kn_3\sqrt{n_2})^{-1/2})\\ &\ll N_4^{1/4}K^{1/2}N_3^{3/2}N_2^{5/4} + N_4^{3/4}N_3^{1/2}N_2^{3/4}.\end{aligned}$$

Then, applying Lemma 5.4 again with $g(t) = 2kn_3\sqrt{n_4 t}$, we see that the same bound holds with the roles of $N_2$ and $N_4$ reversed. Therefore, we have

$$\begin{aligned}\sum_{k\leqslant K}\frac{1}{k}|E_k(N_2,N_3,N_4)| &\ll K^{1/2}N_3^{3/2}\min\{N_2^{5/4}N_4^{1/4},N_2^{1/4}N_4^{5/4}\}+N_3^{1/2}(N_2N_4)^{3/4}\\ &\ll K^{1/2}N_3^{3/2}(N_2N_4)^{3/4}+N_3^{1/2}(N_2N_4)^{3/4}.\end{aligned}$$

□

Combining Lemmas 5.3 and 5.5, we now show that the triple sequence $2n_3\sqrt{n_2n_4}$ is uniformly distributed modulo 1.

THEOREM 5.6. *Let $N_2, N_3, N_4 \geqslant 1$, and $0 \leqslant \alpha < \beta \leqslant 1$. Then*

$$\lim_{N_2N_4\to\infty}\frac{Z_f(N_2,N_3,N_4;\alpha,\beta)}{N_2N_3N_4}=\beta-\alpha.$$

REMARK 5.7. Note that we do not require that each of $N_2$, $N_3$, and $N_4$ tends to infinity in the above limit. Rather, we require only that the product $N_2N_4\to\infty$.

*Proof.* Fix $0<\varepsilon<\frac{1}{16}$. Applying Lemmas 5.3 and 5.5 with $K=(N_2N_4)^{1/4}$, we see that

$$\begin{aligned}\sum_{k\leqslant K}\frac{1}{k}|E_k(N_2,N_3,N_4)| &\ll (N_2N_4)^{3/4+\varepsilon}N_3+\min\{(N_2N_4)^{1+\varepsilon},N_3^{3/2}(N_2N_4)^{7/8}\}\\ &\ll (N_2N_4)^{3/4+\varepsilon}N_3+(N_2N_4)^{15/16+\varepsilon}N_3^{3/4}.\end{aligned}$$

Since (with this same choice of $K$) we have $N_2N_3N_4/K=(N_2N_4)^{3/4}N_3$, using the above bound in Theorem 5.1 yields the theorem. □

*Proof of Theorem* 1.2. Let $F(N_2,N_4)$ be any function tending to infinity with $N_2N_4$ and satisfying the bound

$$F(N_2,N_4)\leqslant\frac{N_1N_2^{1/4}}{18N_3^{1/2}N_4^{1/4}}. \tag{5.2}$$

Without loss of generality, we may assume that $N_2N_4$ is large enough that $F(N_2,N_4)\geqslant 1$. Hence, we may write

$$\#S(N_1,N_2,N_3,N_4)=\#S_1(N_1,N_2,N_3,N_4)+\#S_2(N_1,N_2,N_3,N_4),$$

where

$$\begin{aligned}S_1(N_1,N_2,N_3,N_4)&:=\{(n_1,n_2,n_3,n_4)\in S(N_1,N_2,N_3,N_4):\|2n_3\sqrt{n_2n_4}\|\leqslant 1/F(N_2,N_4)\},\\ S_2(N_1,N_2,N_3,N_4)&:=\{(n_1,n_2,n_3,n_4)\in S(N_1,N_2,N_3,N_4):\|2n_3\sqrt{n_2n_4}\|> 1/F(N_2,N_4)\}.\end{aligned}$$

It follows from Theorem 5.6 that $\#S_1(N_1,N_2,N_3,N_4)=\underline{o}(N_1N_2N_3N_4)$ as $N_2N_4\to\infty$. On the other hand, if $(n_1,n_2,n_3,n_4)\in S_2(N_1,N_2,N_3,N_4)$, then by Proposition 3.1

$$\begin{aligned}N_1\leqslant n_1&<\frac{10n_3^{1/2}n_4^{1/4}}{||2n_3\sqrt{n_2n_4}||n_2^{1/4}}+\frac{1}{n_2^{3/4}n_3^{1/2}n_4^{1/4}}\\ &<\frac{10(2N_3)^{1/2}(2N_4)^{1/4}}{(1/F(N_2,N_4))N_2^{1/4}}+\frac{1}{N_2^{3/4}N_3^{1/2}N_4^{1/4}}\\ &<18F(N_2,N_4)\frac{N_3^{1/2}N_4^{1/4}}{N_2^{1/4}}.\end{aligned}$$

However, this contradicts our choice of $F(N_2, N_4)$ that satisfies (5.2). Therefore, we conclude that $S_2(N_1, N_2, N_3, N_4)$ is empty, and hence $\#S(N_1, N_2, N_3, N_4) = \underline{o}(N_1N_2N_3N_4)$ as $N_2N_4 \to \infty$. □

*Acknowledgements.* We would like to thank J. Achter, P. Clark, E. Goren, A. Harper, A. Silverberg, and J. Wu for useful discussions related to this work. The argument presented in Section 5, which allows us to obtain the result of Theorem 1.2 without any conditions on the relative size of the parameters $N_2, N_3, N_4$, was suggested to us by J. Wu. We are very thankful for his gracious help. We would also like to express our gratitude to the AMS Mathematics Research Communities 2012 program for providing us with the opportunity to work together in a very pleasant working environment and for its generous financial support.

## *References*

**1.** B. Banks, S. Pappalardi and I. Shparlinski, 'On group structures realized by elliptic curves over arbitrary finite fields', *Exp. Math.* 21 (2012) 11–25.
**2.** V. Chandee, C. David, D. Koukoulopoulos and E. Smith, 'Group structures of elliptic curves over finite fields', *Int. Math. Res. Not.* rnt120 (2013).
**3.** C. J. Hillar and D. L. Rhea, 'Automorphisms of finite abelian groups', *Amer. Math. Monthly* 114 (2007) 917–923.
**4.** H. Iwaniec and E. Kowalski, *Analytic number theory*, Colloquium Publications 53 (American Mathematical Society, Providence, RI, 2004).
**5.** E. Krätzel, *Lattice points*, Mathematics and Its Applications (East European Series) 33 (Kluwer Academic Publishers Group, Dordretch/Boston/London, 1988).
**6.** J. Lengler, 'The Cohen–Lenstra heuristic for finite abelian groups', PhD thesis, Universität des Saarlandes, Saarbrucken, Germany, 2009.
**7.** H. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, Regional Conference Series in Mathematics 84 (American Mathematical Society, Providence, RI, 1994).
**8.** H.-G. Rück, 'A note on elliptic curves over finite fields', *Math. Comp.* 49 (1987) 301–304.
**9.** H.-G. Rück, 'Abelian surfaces and jacobian varieties over finite fields', *Compos. Math.* 76 (1990) 351–366.
**10.** S. Rybakov, 'The group of points on abelian varieties over finite fields', *Cent. Eur. J. Math.* 8 (2010) 282–288.
**11.** S. Rybakov, 'The group of points on abelian surfaces over finite fields', *Arithmetic, geometry, cryptography and coding theory*, Contemporary Mathematics 574 (American Mathematical Society, Providence, RI, 2012) 151–158.
**12.** G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics 46 (Cambridge University Press, Cambridge, 1995).
**13.** W. C. Waterhouse, 'Abelian varieties over finite fields', *Ann. Sci. École Norm. Sup.* 4 (1969) 521–560.
**14.** C. Xing, 'The structure of the rational point groups of simple abelian varieties of dimension two over finite fields', *Arch. Math.* 63 (1994) 427–430.
**15.** C. Xing, 'On supersingular abelian varieties of dimension two over finite fields', *Finite Fields Appl.* 2 (1996) 407–421.

*Chantal David*
*Department of Mathematics and Statistics*
*Concordia University*
*1455 de Maisonneuve West*
*Montréal, QC*
*Canada H3G1M8*

cdavid@mathstat.concordia.ca

*Derek Garton*
*Fariborz Maseeh Department of Mathematics and Statistics*
*Portland State University*
*PO Box 751*
*Portland, OR 97207*
*USA*

gartondw@pdx.edu

*Zachary Scherr*
*Department of Mathematics*
*University of Pennsylvania*
*209 South 33rd St.*
*Philadelphia, PA 19104*
*USA*

zscherr@math.upenn.edu

*Arul Shankar*
*Department of Mathematics*
*Harvard University*
*One Oxford St.*
*Cambridge, MA 02138*
*USA*

arul.shnkr@gmail.com

*Ethan Smith*
*Department of Mathematics*
*Liberty University*
*1971 University Boulevard*
*Lynchburg, VA 24502*
*USA*

ecsmith13@liberty.edu

*Lola Thompson*
*Department of Mathematics*
*Oberlin College*
*10 N. Professor St.*
*Oberlin, OH 44074*
*USA*

lola.thompson@oberlin.edu