EVERY FINITE ABELIAN GROUP IS THE GROUP OF RATIONAL POINTS OF AN ORDINARY ABELIAN VARIETY OVER $\mathbb{F}_2$, $\mathbb{F}_3$ AND $\mathbb{F}_5$

STEFANO MARSEGLIA AND CALEB SPRINGER

Abstract. We show that every finite abelian group occurs as the group of rational points of an ordinary abelian variety over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_5$. We produce partial results for abelian varieties over a general finite field $\mathbb{F}_q$. In particular, we show that certain abelian groups cannot occur as groups of rational points of abelian varieties over $\mathbb{F}_q$ when q is large. Finally, we show that every finite cyclic group arises as the group of rational points of infinitely many simple abelian varieties over $\mathbb{F}_2$.

1. Introduction

Recently, Howe and Kedlaya [HK21] proved that every positive integer m is the order of the group of rational points of an ordinary abelian variety over $\mathbb{F}_2$. Shortly afterwards, Van Bommel, Costa, Li, Poonen and Smith [vBCL$^+$21] extended the result to the finite fields $\mathbb{F}_3$ and $\mathbb{F}_5$. Similar results, with some exceptions, are obtained for the finite fields $\mathbb{F}_4$, $\mathbb{F}_7$ and, when m is large enough, for a general finite field $\mathbb{F}_q$. In another direction, Kedlaya expanded the result of [HK21] to prove that every positive integer is the order of the group of rational points of *infinitely many* (not necessarily ordinary) simple abelian varieties over $\mathbb{F}_2$ [Ked21, Theorem 1.1]. The goal of this paper is to strengthen these results from statements regarding cardinality to statements regarding groups.

1.1. **Finite fields of small cardinality.**

For clarity, we start with a simplified statement of our first main result. Recall that an abelian variety A of dimension g over a finite field of characteristic p is called *ordinary*, resp. *almost ordinary*, if the p-torsion of $A(\overline{\mathbb{F}}_p)$ consists of p^g points, resp. p^{g-1}.

Main Theorem 1. *Let G be a finite abelian group. Then the following statements hold.*

(1) *Let k be one of the finite fields $\mathbb{F}_2$, $\mathbb{F}_3$ or $\mathbb{F}_5$. Then there is an ordinary abelian variety A defined over k, such that $A(k) \cong G$.*
(2) *Over $\mathbb{F}_4$, there is an abelian variety B which is either ordinary or almost ordinary such that $B(\mathbb{F}_4) \cong G$.*

In fact, over $\mathbb{F}_2$, the proof of this result also provides a way to bound the dimension of the abelian variety A appearing in the theorem. Moreover, the non-ordinary abelian varieties used over $\mathbb{F}_4$ can be described precisely. The version of the theorem including all details appears in Section 3 as Theorem 3.3.

The outline of the proof of the first part of Main Theorem 1 is as follows. To begin, we reduce to the case when the group G is cyclic, and we focus our attention on isogeny classes with the key property of being *square-free*; see Definition 2.1. Square-free isogeny classes over prime fields $\mathbb{F}_p$ and square-free ordinary isogeny classes over any finite field $\mathbb{F}_q$ are well-understood in terms of fractional ideals in étale algebras over $\mathbb{Q}$; see Definition 2.2 and Proposition 2.5. Using this description, we prove that in every such isogeny class there is an abelian variety with cyclic group of points; see

Date: February 9, 2022.

2020 *Mathematics Subject Classification.* Primary: 14K15. Secondary: 14G15, 11G10.

Key words and phrases. Abelian variety, finite fields, group of rational points.

Marseglia is supported by NWO grant VI.Veni.202.107.

Springer is partially supported by National Science Foundation award CNS-2001470.

Proposition 2.7. Therefore, because the number of rational points on an abelian variety is an isogeny invariant [Tat66, Theorem 1.(c)], we simply require a square-free isogeny class of abelian varieties with the correct number of points. The result of Howe and Kedlaya [HK21] provides the necessary isogeny classes in the case of $\mathbb{F}_2$, and the result of Van Bommel et al. [vBCL$^+$21] does the same for the remaining cases. See Theorems 3.1 and 3.2 for the precise statements of their results. This allows us to conclude the proof of the first part of Main Theorem 1. The second part requires a small modification of the argument since there is no ordinary abelian variety over $\mathbb{F}_4$ with 3 rational points; see [vBCL$^+$21, Remark 1.16]. The argument shows that any finite cyclic group is the group of rational points of a square-free ordinary abelian variety over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_5$; see Corollary 3.5. The same is true over $\mathbb{F}_4$ and $\mathbb{F}_7$, with some exceptions; see again Corollary 3.5 and Corollary 3.6.

1.2. **Finite fields of arbitrary cardinality.** We pause to stress that Propositions 2.5 and 2.7 work over any finite field $\mathbb{F}_q$. Since [vBCL$^+$21] shows that, for any prime power q, every sufficiently large integer is the order of an abelian variety defined over $\mathbb{F}_q$, this gives us the following result.

Main Theorem 2. *Let q be a prime power. If $m_1, \dots, m_r$ are integers satisfying $m_i \geq q^{3\sqrt{q}\log q}$ for all i, then the group $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ is isomorphic to the group of rational points of an ordinary abelian variety over $\mathbb{F}_q$.*

Main Theorem 2 is recalled in Section 4 as Theorem 4.4, together with further discussion about general finite fields. For example, we show that abelian groups of small exponent, regardless of cardinality, never appear as a group of rational points for an abelian variety over $\mathbb{F}_q$ when q is large; see Proposition 4.2.

1.3. **Infinitely many occurrences.** We now return to the finite field $\mathbb{F}_2$. After proving that every positive integer is the order of the group of rational points of infinitely many simple abelian varieties over $\mathbb{F}_2$ [Ked21, Theorem 1.1], Kedlaya suggested that it would be interesting to show an analogous statement regarding groups. The results contained in Section 2 allow us to immediately deduce that every finite cyclic group is the group of rational points of infinitely many simple abelian varieties over $\mathbb{F}_2$; see Proposition 5.2. Using this, we can prove the following stronger statement, which will be recalled in Section 5 as Theorem 5.3.

Main Theorem 3. *For every $n \geq 1$, there is an infinite set of Weil 2-polynomials $\{f_{n,j}(t)\}_{j\geq 1}$ which are pairwise coprime and enjoy the following property. For each j, every finite abelian group of cardinality n arises as the group of rational points of an abelian variety with Weil polynomial $f_{n,j}(t)$.*

However, as noted by Kedlaya, a result of Kadets [Kad21] shows that these results are impossible over $\mathbb{F}_q$ for larger q. Indeed, if $q > 2$, then for each positive integer m there are only finitely many simple abelian varieties with m rational points.

1.4. **Related work.** We conclude this section by outlining additional relevant literature. The groups of points of elliptic curves have been studied extensively, in particular in relation to their application to cryptography; see for example [Rüc87], [TVN07, Theorem 3.3.15], and [Vol88]. The groups of points of abelian surfaces have been studied by Xing in [Xin94] and [Xin96], Rybakov in [Ryb12], and by David et al. in [DGS$^+$14]. Such results were extended to dimension three by Kotelnikova in [Kot19]. Giangreco-Maidana determined precisely when a given Weil polynomial corresponds to a cyclic isogeny class (Definition 2.6) in [GM19, GM20, GM21]. Rybakov provided classification results for the group of points in [Ryb10] and [Ryb15] in terms of the Newton polygon of the characteristic polynomial of Frobenius. The second author gave a classification in terms of the endomorphism ring of the abelian variety in [Spr21].

Acknowledgements. The authors thank Bjorn Poonen, Valentijn Karemaker and Kiran Kedlaya for their helpful comments.

2. The square-free case

Definition 2.1. An isogeny class of abelian varieties over $\mathbb{F}_q$ is called *square-free* if the corresponding characteristic polynomial of Frobenius (also known as its *Weil polynomial*) has no multiple complex roots. An abelian variety A over $\mathbb{F}_q$ is called *square-free* if it belongs to a square-free isogeny class.

Definition 2.2. Let A be an abelian variety over a finite field $\mathbb{F}_q$. We say that A satisfies condition **Ord** if it is ordinary. We say that A satisfies condition **CS** if q is a prime number and the Weil polynomial has no real roots; such abelian varieties were studied by Centeleghe and Stix in [CS15].

Note that in [HK21], an isogeny class is called square-free if the isogeny decomposition has no repeated factors. Their definition differs from ours in general, so we provide the following lemma to disambiguate the use of terminology. For example, we do not call an elliptic curve over $\mathbb{F}_{p^2}$ with Weil polynomial $(x-p)^2$ square-free in this paper even though it is simple.

Lemma 2.3. *Let A be an abelian variety over $\mathbb{F}_q$. The following are equivalent.*

(1) A has square-free Weil polynomial, i.e. A is square-free.

(2) The endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is commutative.

Additionally, these conditions imply the following.

(3) The isogeny decomposition of A contains no repeated factors.

Moreover, if A satisfies **Ord** *or* **CS***, then all three conditions are equivalent. In particular, if A satisfies* **Ord** *or* **CS***, then A is simple if and only if its Weil polynomial is irreducible.*

Proof. The first equivalence is [Tat66, Theorem 2(c)]. The implication that the first two conditions imply the thirds follows from [Tat66, Theorem 1(b)]. For property **Ord**, it follows from Honda-Tate theory that an ordinary isogeny class is simple if and only if its Weil polynomial is irreducible; see for example [How95, Theorem 3.3]. For property **CS**, note that the Weil polynomial of any simple abelian variety over a prime finite field $\mathbb{F}_p$ is irreducible, unless the Weil polynomial has a real root; see for example [Wat69, Theorem 6.1] or [Tat71, p.96]. □

Remark 2.4. Over a prime field $\mathbb{F}_p$, there is only one simple isogeny class whose Weil polynomial has real roots, namely $(x^2-p)^2$.

Square-free abelian varieties satisfying **Ord** or **CS** are well-understood in terms of fractional ideals, thanks to certain equivalences of categories proved by Deligne in [Del69] and Centeleghe-Stix in [CS15]. We summarize the relevant results in the following Proposition; see [Mar21, Cor. 4.4 and Cor. 4.7] for the proofs. Let f_A be the characteristic polynomial of Frobenius for a square-free abelian variety A satisfying **Ord** or **CS**. Let K be the étale algebra generated by the Frobenius endomorphism π, that is, $K = \mathbb{Q}[\pi] = \mathbb{Q}[x]/(f_A)$. Denote by $\mathbb{Z}[\pi, \overline{\pi}]$ the order in K generated by the Frobenius and Verschiebung endomorphisms.

Proposition 2.5. *There is an equivalence*[1] *$\mathcal{F}$ between the category of abelian varieties isogenous to A (with $\mathbb{F}_q$-homomorphisms) and the category of fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals in K (with $\mathbb{Z}[\pi, \overline{\pi}]$-linear morphisms). In particular, if $\mathcal{F}(B) = I$ then we have an isomorphism of finite abelian groups*

$$B(\mathbb{F}_q) \cong \frac{I}{(\pi-1)I}.$$

Before applying this proposition and concluding this section, we recall one more definition.

[1] In the **CS** case, the functor is contravariant. This detail is not needed in this paper.

Definition 2.6. An abelian variety A over $\mathbb{F}_q$ is *cyclic* if $A(\mathbb{F}_q)$ is a cyclic group. An isogeny class is cyclic if every abelian variety in the isogeny class is cyclic.

Using Proposition 2.5, we can prove the existence of cyclic abelian varieties within every isogeny class satisfying **Ord** or **CS**. The following proposition can be viewed as a generalization of a result of Galbraith for elliptic curves [Gal99, Lemma 1].

Proposition 2.7. *Every square-free isogeny class over $\mathbb{F}_q$ satisfying* **Ord** *or* **CS** *contains a cyclic abelian variety*

Proof. We fix a square-free isogeny class over $\mathbb{F}_q$ satisfying **Ord** or **CS**. By Proposition 2.5 there exists an abelian variety A in such an isogeny class such that $\mathcal{F}(A) = \mathbb{Z}[\pi, \overline{\pi}]$. Observe that we have a natural isomorphism $\mathbb{Z}[\pi, \overline{\pi}] \cong \mathbb{Z}[x, y]/(f_A(x), xy - q)$ which sends π to the class of x and $\overline{\pi}$ to the class of y. With this notation, Proposition 2.5 implies that

$$A(\mathbb{F}_q) \cong \frac{\mathbb{Z}[\pi, \overline{\pi}]}{(\pi - 1)} \cong \frac{\mathbb{Z}[x, y]}{(f_A(x), xy - q, x - 1)}.$$

By the division algorithm we can write $f_A(x) = (x - 1)p(x) + f_A(1)$, for some polynomial $p(x)$. This relation together with $y - q = (xy - q) - y(x - 1)$ shows that we have the following equality of ideals of $\mathbb{Z}[x, y]$:

$$(f_A(x), xy - q, x - 1) = (f_A(1), x - 1, y - q).$$

Therefore the evaluation map $(x, y) \mapsto (1, q)$ induces an isomorphism

$$\frac{\mathbb{Z}[x, y]}{(f_A(1), x - 1, y - q)} \cong \frac{\mathbb{Z}}{(f_A(1))}.$$

We conclude that $A(\mathbb{F}_q)$ is a cyclic group. □

Remark 2.8. We note that the same result can be deduced from [Ryb10], and in the simple case, the result can also be deduced from [Spr21, Theorem 1.3]. Our proof shows that we can choose the cyclic ordinary abelian variety A to have endomorphism ring isomorphic to $\mathbb{Z}[\pi, \overline{\pi}]$. In fact, any abelian variety in the given isogeny class with minimal endomorphism ring is cyclic because $\mathbb{Z}[\pi, \overline{\pi}]$ is Gorenstein; see [CS15, Theorem 11].

3. Proof of Main Theorem 1

We now focus on abelian varieties defined over $\mathbb{F}_2$. As indicated in the introduction, Howe and Kedlaya proved the following theorem.

Theorem 3.1 (Theorem 1, [HK21])**.** *Let $m > 0$ and $d > 2$ be integers with $m < (4/3)2^d + 1$. Then there is a square-free ordinary abelian variety A over $\mathbb{F}_2$ of dimension at most d with $m = \#A(\mathbb{F}_2)$.*

Over $\mathbb{F}_3, \mathbb{F}_4$ and $\mathbb{F}_5$, Van Bommel et al. proved the following result.

Theorem 3.2 ([vBCL$^+$21, Theorem 1.13(a), Remarks 1.16 and 1.18])**.** *Let m be a positive integer and k be $\mathbb{F}_3, \mathbb{F}_4$ or $\mathbb{F}_5$. Then there is a square-free abelian variety A over k with $m = \#A(k)$. One can choose A to be ordinary except in the case $m = 3$ and $k = \mathbb{F}_4$.*

We are now ready to complete the proof of Main Theorem 1.

Theorem 3.3. *Let*

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

be a finite abelian group. The following statements hold.

- *Let k be one of the finite fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$. Then there is an ordinary abelian variety A defined over k, such that $A(k) \cong G$;*

- *There is an abelian variety B over $\mathbb{F}_4$, such that $B(\mathbb{F}_4) \cong G$ and B is either ordinary or of the form $B \cong B' \times E$ where B' is ordinary and E belongs to the unique isogeny class of supersingular elliptic curves over $\mathbb{F}_4$ with 3 rational points; see the LMFDB label* [LMF21, 1.4.ac]. *The variety B can be taken to be ordinary unless G is a 3-group such that $G \cong (\mathbb{Z}/3\mathbb{Z})^{n_1} \times \prod_{j>1}(\mathbb{Z}/3^j\mathbb{Z})^{n_j}$ for n_1 odd.*

Moreover, if $k = \mathbb{F}_2$ and $d_1, \ldots, d_r$ are integers satisfying $n_j < (4/3)2^{d_j} + 1$ and $d_j \geq 3$ for each $1 \leq j \leq r$, then there is an ordinary abelian variety A defined over $\mathbb{F}_2$ of dimension at most $d = d_1 + \cdots + d_r$ such that $A(\mathbb{F}_2) \cong G$.

Proof. Assume that k is one of the finite fields $\mathbb{F}_2$, $\mathbb{F}_3$, or $\mathbb{F}_5$. We can immediately reduce to the case when $r = 1$, that is, when the group G is cyclic. By Theorems 3.1 and 3.2, there exists a square-free ordinary isogeny class over k with $|G|$ rational points. By Proposition 2.7, we have an abelian variety A within this isogeny class with cyclic group of points, that is, we have $A(k) \cong G$.

We deal now with the finite field $\mathbb{F}_4$. Consider the simple ordinary isogeny class of abelian surfaces over $\mathbb{F}_4$ with 9 rational points given by the Weil polynomial $x^4 - 3x^3 + 7x^2 - 12x + 16$; see the LMFDB label [LMF21, 2.4.ad_h]. Let $K = \mathbb{Q}(\pi)$ be the endomorphism algebra of this isogeny class and let $\mathcal{O}_K$ be the maximal order of K. We observe that

$$\frac{\mathcal{O}_K}{(\pi - 1)\mathcal{O}_K} \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Hence by Proposition 2.5, in this isogeny class there is an abelian surface B_0 with group of rational points isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$. Let E belong to the unique isogeny class of supersingular elliptic curves over $\mathbb{F}_4$ with 3 rational points; see the LMFDB label [LMF21, 1.4.ac].

Write the group G as a product of cyclic groups

$$G \cong (\mathbb{Z}/3\mathbb{Z})^{2e+\delta} \times (\mathbb{Z}/s_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/s_f\mathbb{Z})$$

where $\delta \in \{0, 1\}$, $e \geq 0$ and either $s_j = 2$ or $s_j > 3$ for all j. Using Theorem 3.2 with the method from above, we can find an ordinary abelian variety B_1 over $\mathbb{F}_4$ whose group of rational points is isomorphic to $(\mathbb{Z}/s_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/s_f\mathbb{Z})$. If G is not a 3-group then there exists an s_j which is not divisible by 3, say s_1. Again, the above construction using Theorem 3.2 gives us an ordinary abelian variety B_1' over $\mathbb{F}_4$ whose group of rational points is isomorphic to $(\mathbb{Z}/3s_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/s_f\mathbb{Z})$.

With this set up, we now distinguish three cases. If $\delta = 0$ then we set $B = B_0^e \times B_1$. If $\delta = 1$ and G is not a 3-group then set $B = B_0^e \times B_1'$. Finally, if $\delta = 1$ and G is a 3-group then we set $B = E^\delta \times B_0^e \times B_1$. In all three cases, we have that $B(\mathbb{F}_4) \cong G$ by construction and the Chinese Remainder Theorem. In the first two cases, the variety B is ordinary, while in the last one B is almost ordinary. □

Remark 3.4. We stress that Theorem 3.3 does not exclude the existence of ordinary abelian varieties over $\mathbb{F}_4$ with group of points isomorphic to $(\mathbb{Z}/3\mathbb{Z})^{n_1} \times \prod_{j>1}(\mathbb{Z}/3^j\mathbb{Z})^{n_j}$ for n_1 odd. Indeed, the LMFDB [LMF21] contains ordinary abelian varieties over $\mathbb{F}_4$ with group of points $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$; for example, see the isogeny class with label [LMF21, 2.4.b_f]. However, the LMFDB does not currently contain any ordinary abelian varieties over $\mathbb{F}_4$ with a group of rational points isomorphic to $(\mathbb{Z}/3\mathbb{Z})^{2e+1}$ for $e \geq 1$. Nonexistence when $e = 0$ follows from [Kad21, Theorem 3.2]; see [vBCL+21, Remark 1.16]. Proving more general existence or nonexistence results will require additional understanding of which groups can occur as the group of rational points of an abelian variety in a given isogeny class.

From the proof of Theorem 3.3 we immediately deduce the following special case.

Corollary 3.5. *Let k be one of the finite fields $\mathbb{F}_2$, $\mathbb{F}_3$ or $\mathbb{F}_5$. Let G be a finite cyclic abelian group. Then there are*

- *a square-free ordinary abelian variety A over k with $A(k) \cong G$; and*
- *a square-free abelian variety B over $\mathbb{F}_4$ with $B(\mathbb{F}_4) \cong G$, which we can choose to be ordinary if $G \neq \mathbb{Z}/3\mathbb{Z}$.*

In a similar fashion, using [vBCL$^+$21, Theorem 1.13(a), Remarks 1.17 and 1.18], we can achieve a result analogous to Corollary 3.5 for abelian varieties over the finite field $\mathbb{F}_7$.

Corollary 3.6. *Let G be a finite cyclic abelian group with $|G| \notin \{2, 8, 14, 16, 17, 73\}$. Then there is a square-free ordinary abelian variety A over $\mathbb{F}_7$ with $A(\mathbb{F}_7) \cong G$.*

Remark 3.7. Using Proposition 2.7 or Remark 2.8, one can construct square-free abelian varieties over $\mathbb{F}_7$, necessarily non-ordinary, with group of rational points isomorphic to $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/73\mathbb{Z}$.

4. Proof of Main Theorem 2

For large q, the Weil bounds prohibit the existence of abelian varieties over $\mathbb{F}_q$ with a relatively small number of points; see [Wei48] and [Kad21]. However, in [vBCL$^+$21] it is proven that:

Theorem 4.1 ([vBCL$^+$21, Theorem 1.13(b), Remarks 1.16 and 1.18])**.** *For an arbitrary prime power q, every integer $m \geq q^{3\sqrt{q}\log q}$ arises as $m = \#A(\mathbb{F}_q)$ for some ordinary square-free abelian variety A over $\mathbb{F}_q$.*

Still, Theorem 4.1 does not imply that every abelian group of sufficiently large order arises as the group of points of an abelian variety over $\mathbb{F}_q$, as shown by the following proposition, which was suggested by Bjorn Poonen.

Proposition 4.2. *Let $m > 1$ be an integer and q a power of a prime p. Suppose there exists an abelian variety A over $\mathbb{F}_q$ such that $A(\mathbb{F}_q)$ is a group of exponent m. Then we have the following.*

(1) Unconditionally, $q \leq (m+1)^2$;
(2) If m is also a power of p, then we have $q \leq (\sqrt{m}+1)^2$.

Proof. Suppose that g is the dimension of A. Then, using the Weil bounds and the structure of torsion subgroups, we get

$$(\sqrt{q}-1)^{2g} \leq \#A(\mathbb{F}_q) \leq \#A(\overline{\mathbb{F}}_q)[m] \leq m^{2g}.$$

Rearranging, we obtain $q \leq (m+1)^2$. The stricter upper bound follows similarly by using the structure of the p^e-torsion of an abelian variety in characteristic p. □

Corollary 4.3. *If $q > 9$ or $q = 8$, then the group $(\mathbb{Z}/2\mathbb{Z})^r$ for $r \geq 1$ does not arise as the group of rational points for any abelian variety over $\mathbb{F}_q$.*

The following theorem, whose proof is exactly like that of Theorem 3.3, is the best that can be obtained with our current methods. The nonexistence results above show that restrictions on the sizes of the cyclic factors are necessary. We observe that there are some finite abelian groups which are not outlawed by Proposition 4.2 but which are also not realized in Theorem 4.4. For general q, determining which of these groups arise as the group of rational points of an ordinary abelian variety over $\mathbb{F}_q$ remains an open question for future research.

Theorem 4.4. *Let q be a prime power. If $m_1, \ldots, m_r$ are integers satisfying $m_i \geq q^{3\sqrt{q}\log q}$ for all i, then the group $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ is isomorphic to the group of rational points of an ordinary abelian variety over $\mathbb{F}_q$.*

In the previous section, we deduced that certain cyclic groups can be realized as the group of rational points of a square-free abelian variety over $\mathbb{F}_q$ for various small values of q; see Corollaries 3.5 and 3.6. For arbitrary q, we prove an analogous corollary concerning square-free abelian varieties with an explicit bound for the size of the group.

Corollary 4.5. *Fix a prime power q and let m be an integer satisfying $m \geq q^{3\sqrt{q}\log q}$. Then there is a square-free ordinary abelian variety over $\mathbb{F}_q$ whose group of rational points is isomorphic to $\mathbb{Z}/m\mathbb{Z}$.*

Alternatively, we prove the following result concerning *geometrically simple* abelian varieties. As a trade-off for this stronger condition on the abelian variety, there is no effective lower bound for the size of the group in the following theorem.

Theorem 4.6. *Fix a prime power q and let n be sufficiently large with respect to q. There is a geometrically simple ordinary abelian variety A over $\mathbb{F}_q$ with $A(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. When n is sufficiently large, another result [vBCL+21, Corollary 1.3] from the same paper as Theorem 4.1 proves that there is a geometrically simple ordinary abelian variety A_0 over $\mathbb{F}_q$ with $|A_0(\mathbb{F}_q)| = n$. By Proposition 2.7, there is an abelian variety A isogenous to A_0 which is cyclic, which concludes the theorem. □

5. Proof of Main Theorem 3

The goal of this section is to prove Main Theorem 3. As a foundation, we have the following result of Kedlaya regarding cardinality.

Theorem 5.1 (Theorem 1.1, [Ked21]). *Every positive integer is equal to the order of the group of rational points of infinitely many simple abelian varieties (of various dimensions) over $\mathbb{F}_2$.*

Using this result together with Lemma 2.3, Remark 2.4 and Proposition 2.7, we can immediately prove the following result.

Proposition 5.2. *Let $n \geq 1$ be a positive integer. There are infinitely many simple abelian varieties A over $\mathbb{F}_2$ with $A(\mathbb{F}_2) \cong \mathbb{Z}/n\mathbb{Z}$.*

When searching for examples of (possibly non-simple) abelian varieties A over $\mathbb{F}_2$ such that $A(\mathbb{F}_2)$ is isomorphic to a given finite abelian group G, there is one way to "cheat" to find an infinite number of examples: Find one example A_0 with $A_0(\mathbb{F}_2) \cong G$ using Theorem 3.3, then consider the infinite set $\{A_0 \times B \mid \#B(\mathbb{F}_2) = 1\}$. The fact that there are infinitely many abelian varieties B over $\mathbb{F}_2$ with only one point is a special case of Kedlaya's theorem which was originally proven by Madan and Pal [MP77]. In order to prove the existence of genuinely interesting infinite storehouses of examples, we find examples with pairwise coprime Weil polynomials. This corresponds to finding examples whose isogeny classes share no simple factors in common. We now prove Main Theorem 3.

Theorem 5.3. *For every $n \geq 1$, there is an infinite set of Weil 2-polynomials $\{f_{n,j}(t)\}_{j\geq 1}$ which are pairwise coprime and enjoy the following property. For each j, every finite abelian group of cardinality n arises as the group of rational points of an abelian variety with Weil polynomial $f_{n,j}(t)$.*

Proof. Write $n = \ell_1 \dots \ell_r$, where $\ell_1, \dots, \ell_r$ are primes that are not necessarily distinct. By Proposition 5.2, for each $1 \leq i \leq r$, there are infinitely many simple abelian varieties A_i over $\mathbb{F}_2$ such that $A_i(\mathbb{F}_2) \cong \mathbb{Z}/\ell_i\mathbb{Z}$. By Remark 2.4, there is only one simple isogeny class over $\mathbb{F}_2$ whose Weil polynomial has real roots; see [LMF21, 2.2.a_ae]. Hence, by Lemma 2.3, we can choose the A_i to have distinct irreducible Weil polynomial. Let $\mathcal{C}$ be the isogeny class of $A_1 \times \dots \times A_r$. Note that $\mathcal{C}$ is square-free by construction.

Because each sub-product $\prod_{j\in S} A_j$ for $S \subset \{1, \dots, r\}$ is also square-free, we can apply Proposition 2.7 to get a cyclic isogenous variety A_S satisfying $A_S(\mathbb{F}_2) \cong \mathbb{Z}/(\prod_{j\in S} \ell_j)\mathbb{Z}$. In this way, we obtain all abelian groups of cardinality n as the group of rational points of an abelian variety in $\mathcal{C}$. □

Remark 5.4. With the currently technology we are not able to determine whether given an arbitrary finite abelian group G there are infinitely many *simple* abelian varieties over $\mathbb{F}_2$ with group of rational points isomorphic to G. A possible approach to this questions is to study which groups can occur in a given isogeny class.

References

[vBCL$^+$21] Raymond van Bommel, Edgar Costa, Wanlin Li, Bjorn Poonen, and Alexander Smith, *Abelian varieties of prescribed order over finite fields*, arXiv e-prints (2021), arXiv:2106.13651.

[CS15] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$*, Algebra Number Theory **9** (2015), no. 1, 225–265. MR 3317765

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243. MR 0254059

[DGS$^+$14] Chantal David, Derek Garton, Zachary Scherr, Arul Shankar, Ethan Smith, and Lola Thompson, *Abelian surfaces over finite fields with prescribed groups*, Bull. Lond. Math. Soc. **46** (2014), no. 4, 779–792. MR 3239616

[Gal99] Steven D. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS J. Comput. Math. **2** (1999), 118–138. MR 1728955

[GM19] Alejandro J. Giangreco-Maidana, *On the cyclicity of the rational points group of abelian varieties over finite fields*, Finite Fields Appl. **57** (2019), 139–155. MR 3921286

[GM20] ______, *Local cyclicity of isogeny classes of abelian varieties defined over finite fields*, Finite Fields Appl. **62** (2020), 101628, 9. MR 4053144

[GM21] ______, *Corrigendum to "Local cyclicity of isogeny classes of abelian varieties defined over finite fields" [Finite Fields Appl. 62 (2020) 101628]*, Finite Fields Appl. **69** (2021), 101703, 2. MR 4183334

[HK21] Everett W. Howe and Kiran S. Kedlaya, *Every positive integer is the order of an ordinary abelian variety over $\mathbb{F}_2$*, Research in Number Theory **7** (2021), no. 4, 59.

[How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401. MR 1297531

[Kad21] Borys Kadets, *Estimates for the number of rational points on simple abelian varieties over finite fields*, Math. Z. **297** (2021), no. 1-2, 465–473. MR 4204701

[Ked21] Kiran S. Kedlaya, *Abelian varieties over $\mathbb{F}_2$ of prescribed order*, arXiv e-prints (2021), arXiv:2107.12453.

[Kot19] Yulia Kotelnikova, *Groups of points on abelian threefolds over finite fields*, Finite Fields Appl. **58** (2019), 177–199. MR 3947815

[LMF21] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, 2021, [Online; accessed 20 July 2021].

[Mar21] Stefano Marseglia, *Computing square-free polarized abelian varieties over finite fields*, Math. Comp. **90** (2021), no. 328, 953–971. MR 4194169

[MP77] Manohar L. Madan and Sat Pal, *Abelian varieties and a conjecture of R. M. Robinson*, J. Reine Angew. Math. **291** (1977), 78–91. MR 439848

[Rüc87] Hans-Georg Rück, *A note on elliptic curves over finite fields*, Math. Comp. **49** (1987), no. 179, 301–304. MR 890272

[Ryb10] Sergey Rybakov, *The groups of points on abelian varieties over finite fields*, Cent. Eur. J. Math. **8** (2010), no. 2, 282–288. MR 2610753

[Ryb12] ______, *The groups of points on abelian surfaces over finite fields*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, pp. 151–158. MR 2961407

[Ryb15] ______, *On classification of groups of points on abelian varieties over finite fields*, Mosc. Math. J. **15** (2015), no. 4, 805–815. MR 3438835

[Spr21] Caleb Springer, *The structure of the group of rational points of an abelian variety over a finite field*, European Journal of Mathematics (2021), 1–13.

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR 0206004

[Tat71] ______, *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

[TVN07] Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs, vol. 139, American Mathematical Society, Providence, RI, 2007. MR 2339649

[Vol88] J. F. Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France **116** (1988), no. 4, 455–458 (1989). MR 1005390

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR 0265369

[Wei48] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], No. 1041, Hermann et Cie., Paris, 1948, Publ. Inst. Math. Univ. Strasbourg **7** (1945). MR 0027151

[Xin94] Chaoping Xing, *The structure of the rational point groups of simple abelian varieties of dimension two over finite fields*, Arch. Math. (Basel) **63** (1994), no. 5, 427–430. MR 1300737

[Xin96] ———, *On supersingular abelian varieties of dimension two over finite fields*, Finite Fields Appl. **2** (1996), no. 4, 407–421. MR 1409453

Mathematical Institute, Utrecht University, P.O. Box 80010, 3508 TA, Utrecht, The Netherlands
Email address: `s.marseglia@uu.nl`

Department of Mathematics, University College London, Gower Street, London WC1H 0AY, UK, and The Heilbronn Insitute for Mathematical Research, Bristol, UK
Email address: `c.springer@ucl.ac.uk`