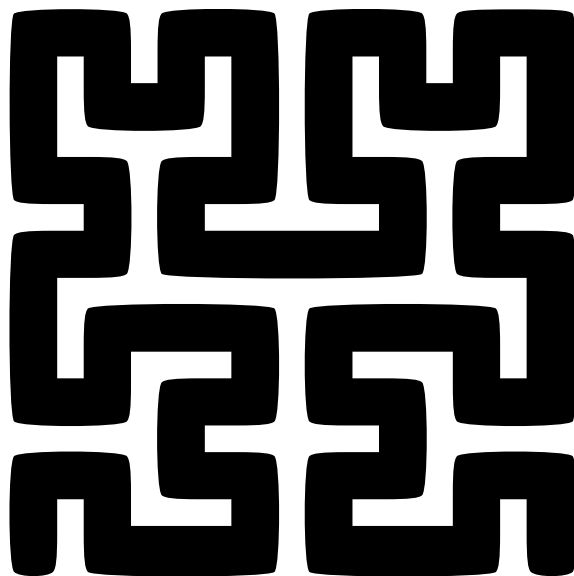




Polynesian Journal of Mathematics

Volume 4, Issue 1

Special volume AĴAX in honor of René Schoof

**Abelian varieties over $\mathbb{F}_2$
of prescribed order and dimension**

Kiran S. Kedlaya

Received 5 Oct 2025

Revised 5 Mar 2026

Accepted 9 Mar 2026

Published 28 Sep 2026

Communicated by Samuele Anni

DOI: 10.69763/polyjmath.4.1

Abelian varieties over $\mathbb{F}_2$ of prescribed order and dimension

Kiran S. Kedlaya

Department of Mathematics, University of California San Diego, United States of America

Abstract

In a previous paper, we showed that for any fixed positive integer m , there exist infinitely many isogeny classes of simple abelian varieties over $\mathbb{F}_2$ whose group of rational points has order m . Here we show that for m even or an odd prime or prime power, for every sufficiently large (depending on m) positive integer g , there is a simple abelian variety of dimension g over $\mathbb{F}_2$ whose group of rational points has order m . This uses a result on recurrent sequences of interlaced polynomials which is presented independently in an appendix.

1 Introduction

The purpose of this paper is to build upon the following theorem proved in [3].

Theorem 1.1. *For every positive integer m , there exist infinitely many isogeny classes of simple abelian varieties A over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = m$.*

Here, we address the following more refined conjecture.

Conjecture 1.2. *For every integer $m > 1$, for every sufficiently large (depending on m) positive integer g , there exists a simple abelian variety A of dimension g over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = m$.*

The case $m = 1$ is omitted because the classification of simple abelian varieties of order 1 (see [7]) shows that if $g > 3$ is not in the image of the Euler totient function, then there is no simple abelian variety A of dimension g over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = 1$.

Our main result towards Conjecture 1.2 is the following theorem. The dependence of “sufficiently large” on m can in principle be made explicit, but we have not consistently done so; see Remark 7.3 for more discussion.

Theorem 1.3. *Conjecture 1.2 holds whenever m is even or a power of an odd prime.*

The author was supported by NSF (grant DMS-2401536) and UC San Diego (Warschawski professorship).

Proof. See Theorem 7.1 for $m = 2$; Theorem 7.2 for $m = 20$; Theorem 8.2 for $m = 3$; Theorem 8.6 for $m = 5, 11, 13, 19$; Theorem 9.1 for $m = 4, 8$; Theorem 9.3 for $m = 9, 25, 27, 49, 81$; Theorem 10.5 for m even with $m \notin \{2, 4, 8, 20\}$; Theorem 11.12 for m odd prime with $m \notin \{3, 5, 11, 13, 19\}$; Theorem 12.3 for m a power of a prime $p > 7$; and Theorem 12.5 for m a power of a prime $p \in \{3, 5, 7\}$ with $m > 100$.

Note that some of the arguments are heavily computer-assisted; the relevant calculations in SageMath 10.6 can be found in a Jupyter notebook associated with this paper and available online at:

<https://kskedlaya.org/papers/construction2.ipynb>

□

Before discussing in more detail the proof of Theorem 1.3, we briefly recall the methodology used in [3] to prove Theorem 1.1. Via the Honda–Tate theorem, the claim translates into a statement about the existence of certain irreducible polynomials over $\mathbb{Z}$ with fixed constant term having all roots in a fixed interval (see Lemma 2.1). The process for constructing these starts with a monic integer polynomial $Q(z)$ with $Q(2) = m$ having all roots in the disc $|z| < \sqrt{2}$; this then gives rise to a second-order linear recurrent sequence whose terms correspond to abelian varieties of order m . By enforcing a suitable condition on the mod-2 reduction of Q , one can then ensure that the terms of this sequence admit infinitely many distinct irreducible factors corresponding to abelian varieties of order m .

To prove Theorem 1.3, we use a similar strategy with a few refinements. First, we observe that the recurrence relation used in [3], whose solutions increase by 2 at each step, admits a “square root”: its terms occur as alternating terms in another second-order linear recurrent sequence (defined by (3.1)) in which the degree increases by 1 at each step, and the desired properties of the roots and constant terms are preserved. On the side of abelian varieties, this means that we produce a sequence of abelian varieties representing every sufficiently large dimension; this gives us the chance to prove Conjecture 1.2 for a given m by showing that all but finitely many polynomials in the resulting sequence are irreducible. For m even, this can again be achieved by some simple 2-adic considerations.

For m odd, the strategy used in [3] to restrict the factorization of polynomials in the recurrent sequence is wholly inadequate for proving Conjecture 1.2, as it only applies to a very sparse subsequence. When m is prime, though, the factorizations are already heavily restricted: any nontrivial factorization involves an abelian variety of order 1, for which we have a complete classification as noted above. This means we can again use mod-2 considerations to eliminate such factorizations and prove Conjecture 1.2. When m is a power of an odd prime p , we can use a similar strategy by augmenting with some simple consideration of the p -adic Newton polygon.

One additional complication compared to [3] is that in both the even case and the odd prime power case, we must impose somewhat stronger mod-2 restrictions on the seed polynomial Q , with the result that a few small cases are missed: from the given proof of Theorem 1.3, we see that the cases

$$m \in \{2, 3, 4, 5, 8, 9, 11, 13, 19, 25, 27, 49, 81\}$$

all require separate handling. These use bespoke constructions based on the following extension of the method of [3]: in place of building a recurrent sequence for the relation (3.1) from a seed polynomial $Q(z)$ which governs the roots of polynomials in the sequence, we can instead give conditions on the first two terms of the sequence that suffice to ensure the correct root placement for all subsequent terms (Theorem 6.2). This amounts to a statement about interlacing polynomials which may be of independent interest (particularly in combinatorics), so we have placed the proof in an appendix which can be read separately from the rest of the paper.

We conclude with a word about the remaining cases of Conjecture 1.2, namely when m is odd and not a prime power (e.g., $m = 15$ or $m = 21$). For such cases, it may be necessary to give up on the methodology of producing a single recurrent sequence whose terms can all be shown to be irreducible, as there seems to be no practical strategy for enforcing this. Instead, it is probably more productive to try to prove the existence of “many” abelian varieties of order m and dimension g , and then argue that most of these must be simple. In this direction, see [4] for discussion of the asymptotic properties of the set of simple abelian varieties with extremely small order compared to their dimension.

2 Setup

We begin by setting up in the manner of [3, § 2], but with some changes in notation especially with regard to indexing.

Lemma 2.1 ([3, Lemma 2.1]). *Let $P(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial of degree d with all roots in $[a, b] := [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and set*

$$R(x) := (-x)^d P(3 - x - 2x^{-1}).$$

Then $R(x)$ occurs as the characteristic polynomial of Frobenius of some simple abelian variety A of dimension d over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = (-1)^d P(0)$.

For $n \geq 0$, let T_n be the Chebyshev polynomial normalized so that $T_n(2 \cos \theta) = 2 \cos n\theta$, and set

$$f_{2n}(x) := x^n T_n(x + x^{-1} - 4); \quad (2.2)$$

this corresponds to $f_n(x)$ in the notation of [3]. Translating [3, (3.2)] into our present notation yields

$$f_{2n}(x) - (x^2 - 4x + 1)f_{2(n-1)}(x) + x^2 f_{2(n-2)}(x) = 0 \quad (n \geq 2). \quad (2.3)$$

From (2.3) and the cases $f_0(x) = 2$, $f_1(x) = x^2 - 4x + 1$ of (2.2), we see that

$$f_{2n}(1) = (-1)^n 2;$$

consequently, there exists a polynomial $f_{2n-1}(x)$ such that

$$f_{2n}(x) - (x - 1)f_{2n-1}(x) + x f_{2n-2}(x) = 0 \quad (n \geq 2). \quad (2.4)$$

Note that

$$f_0(x) = 2, \quad f_1(x) = x - 1, \quad f_2(x) = x^2 - 4x + 1, \quad (2.5)$$

and for $n > 1$ the polynomial $f_n(x)$ is monic of degree n .

Combining (2.3) with two applications of (2.4), we obtain

$$f_{2n-1}(x) - (x-1)f_{2n-2}(x) + xf_{2n-3}(x) = 0 \quad (n \geq 2).$$

Together with (2.4), this asserts that

$$f_n(x) - (x-1)f_{n-1}(x) + xf_{n-2}(x) = 0 \quad (n \geq 2). \quad (2.6)$$

Using the recursion (2.6) and the initial conditions (2.5), we may verify various additional properties of the polynomials f_n , such as the evaluations at special points:

$$f_n(0) = (-1)^n \quad (n > 0) \quad (2.7)$$

$$f_n(1) = i^n + (-i)^n = \begin{cases} 0 & n \equiv 1 \pmod{2} \\ (-1)^{n/2} & n \equiv 0 \pmod{2} \end{cases} \quad (2.8)$$

$$f_n(3 \pm 2\sqrt{2}) = 2(1 \pm \sqrt{2})^n; \quad (2.9)$$

and some symmetries and congruences:

$$f_n(x) = (-x)^n f_n(1/x) \quad (2.10)$$

$$f_n(x) \equiv x^n + 1 + 2n(x^{n-1} + \cdots + x + 1) \pmod{4}. \quad (2.11)$$

3 Polynomials in a recurrent sequence

We record a few algebraic properties of sequences of polynomials satisfying the second-order linear recurrence relation

$$P_n(x) - (x-1)P_{n-1}(x) + xP_{n-2}(x) = 0. \quad (3.1)$$

This includes the example $P_n = f_n$ thanks to (2.6), as well as additional examples to follow.

Remark 3.2. For any sequence $\{P_n(x)\}_n$ of polynomials as in (3.1), we have $P_n(1) = -P_{n-2}(1)$, and so the sequence $\{P_n(1)\}$ is periodic of order dividing 4. This can be used empirically to detect whether a particular polynomial is likely to occur as a deep term in such a sequence.

Before continuing, define the ring

$$R := \frac{\mathbb{Z}[x^\pm, (x-1)^{-1}, w]}{(w^2 - (x-1)w + x)} \cong \mathbb{Z} \left[x^\pm, (x-1)^{-1}, \frac{x-1 + \sqrt{x^2 - 6x + 1}}{2} \right]; \quad (3.3)$$

this is similar to but not quite the ring defined¹ in [3, (2.2)]. In the ring R , the element $y := w^2x^{-1}$ satisfies

$$x + x^{-1} - 4 = y + y^{-1}. \quad (3.4)$$

For any sequence satisfying (3.1), we can find $P_+, P_- \in R$ such that

$$P_n(x) = P_+ w^n + P_-(x - 1 - w)^n \quad (n \geq n_0). \quad (3.5)$$

For example, for $P_n(x) = f_n(x)$ we may take $P_+ = P_- = 1$ and write

$$f_n(x) = w^n + (x - 1 - w)^n. \quad (3.6)$$

When (3.1) holds and $\deg(P_n) = n$, the coefficient of x^{n-1} in P_n equals the coefficient of x^{n-2} in P_{n-1} minus 1. The following lemma is a vast generalization of this.

Lemma 3.7. *Let $\{P_n(x)\}_{n \geq n_0}$ be a sequence of integer polynomials satisfying (3.1), such that P_n is monic of degree n for all $n \geq n_0$. Set $R_n(x) := (-x)^n P_n(3 - x - 2x^{-1})$. Then for $n > n_0$,*

$$R_n(x) - (x^2 - x)R_{n-1}(x) = (2 - x)^{n-n_0-1}(R_{n_0+1}(x) - (x^2 - x)R_{n_0}(x)).$$

In particular,

$$\deg(R_n(x) - (x^2 - x)R_{n-1}(x)) = n - n_0 - 1 + \deg(R_{n_0+1}(x) - (x^2 - x)R_{n_0}(x)).$$

Proof. The recurrence (3.1) translates into

$$R_n(x) - (x^2 - 2x + 2)R_{n-1}(x) - x(x - 1)(x - 2)R_{n-2}(x) = 0,$$

which we rewrite as

$$R_n(x) - (x^2 - x)R_{n-1}(x) + (x - 2)(R_{n-1}(x) - (x^2 - x)R_{n-2}(x)) = 0.$$

This immediately yields the claim. $\square$

Corollary 3.8. *With notation as in Lemma 3.7, set*

$$c := \deg(R_{n_0+1}(x) - (x^2 - x)R_{n_0}(x)).$$

Then for $n \geq n_0$ and $i = 1, \dots, n + n_0 - c$, the i^{th} power sum of $R_n(x)$ equals 1 plus the i^{th} power sum of R_{n-1} .

Proof. We have $\deg(R_n(x)) = 2 \deg(P_n(x)) = 2n$ and by Lemma 3.7, $\deg(R_n(x) - (x^2 - x)R_{n-1}(x)) = n - n_0 - 1 + c$. This means that $R_n(x)$ and $(x^2 - x)R_{n-1}(x)$ agree in their first $2n - (n - n_0 + c)$ coefficients beyond the leading coefficient, which means that the i^{th} power sums agree for $i = 1, \dots, n + n_0 - c$. Since every power sum of $(x^2 - x)R_{n-1}(x)$ is 1 more than the corresponding power sum of $R_{n-1}(x)$, this yields the claim. $\square$

¹We note a typo in [3, (2.2)]: the two presentations only coincide after inverting 2. The presentation on the left is the intended one.

Remark 3.9. In the case where $P_n(x)$ has roots in $[a, b]$ for $n \geq n_0$, we can apply Lemma 2.1 to construct an abelian variety A_n over $\mathbb{F}_2$ with Frobenius characteristic polynomial $R_n(x)$. Corollary 3.8 asserts that for i in the indicated range, the i^{th} Frobenius traces of A_n and A_{n-1} differ by 1; this can be used empirically to identify pairs of terms which lie deep in a recurrent sequence of the form (3.1).

We expand upon [3, Lemma 5.1] in order to control factors of polynomials in a sequence satisfying (3.1). This amounts to inspecting the classification of abelian varieties of order 1 over $\mathbb{F}_2$ [7].

Lemma 3.10. *Let $\{P_n(x)\}_{n \geq 0}$ be a sequence of monic integer polynomials satisfying (3.1). Suppose that $\alpha \in \mathbb{C}^\times$ is a root of both $P_n(x)$ and $P_{n'}(x)$ for some $n < n'$, but not for all n .² Then α is a unit in the ring of algebraic integers.*

Proof. Choose a specialization homomorphism $\pi: R \rightarrow \mathbb{C}$ taking x to α , then set $\gamma := \pi(w)$; note that γ and $\alpha - 1 - \gamma$ are both nonzero because their product is $\alpha \neq 0$. Writing $P_n(x)$ in the form (3.5), noting that $\pi(P_+)$ and $\pi(P_-)$ are not both zero (as otherwise $P_n(\alpha) = 0$ for all n), then solving the system of equations $\pi(P_n(x)) = \pi(P_{n'}(x)) = 0$ yields

$$\gamma^{n'-n} = (\alpha - 1 - \gamma)^{n'-n}.$$

For the polynomials $f_n(x)$ introduced in §2, by writing

$$f_n(x) = w^n + (x - 1 - w)^n$$

we deduce that $\pi(f_{n'-n}(x)) = 2\gamma^{n'-n}$, $\pi(f_{2(n'-n)}(x)) = 2\gamma^{2(n'-n)}$. In particular, α is a root of the polynomial $2f_{2(n'-n)}(x) - f_{n'-n}(x)^2$ which is monic of degree $2(n' - n)$ with constant term 1. $\square$

Lemma 3.11. *Let $\{P_n(x)\}_{n \geq 0}$ be a sequence of monic integer polynomials satisfying (3.1). Suppose that α is a unit in the ring of algebraic integers and a root of $P_n(x)$ for some n (but not all n).*

- (a) *There exist integers $k > 1$ and $r \in \{0, \dots, k-1\}$ for which $P_{n'}(\alpha) = 0$ if and only if $n' \equiv r \pmod{k}$.*
- (b) *Let $S(x)$ be the minimal polynomial of α over $\mathbb{Q}$. If $k \notin \{7, 30\}$, then $S(x) \equiv \Phi_k(x) \pmod{2}$; otherwise, $S(x)$ reduces to one of the two irreducible factors of $\Phi_k(x) \pmod{2}$. (See Table 1 for some of the values of $S(x)$ for small k .)*

Proof. Choose π as in the proof of Lemma 3.10. As in [7], the fact that α is a unit in the ring of algebraic integers means that $\alpha + \alpha^{-1} - 4$ is an algebraic integer with all conjugates in $[-2, 2]$, and hence of the form $\zeta + \zeta^{-1}$; per (3.4), this means that $\zeta := \gamma^2 \alpha^{-1} = \pi(y)$ is a root of unity. Let k be the order of ζ .

Writing P_n in the form (3.5) and replacing $\alpha - 1 - \gamma$ with $\alpha/\gamma = \gamma\zeta$, we have

$$0 = \pi(P_+)\gamma^n + \pi(P_-)(\alpha - 1 - \gamma)^n = \pi(P_+)\gamma^n + \pi(P_-)\gamma^n\zeta^{-n},$$

so $\pi(P_+/P_-) = -\zeta^{-n}$. Let r be the remainder upon dividing n by k ; for this choice of k and r , we have (a).

²The “not for all n ” clause should have also been included in [3, Lemma 5.1].

k	$S(x)$	γ	α	γ^2/α
2	$x - 1$	ζ_4	1	-1
4	$x^2 - 4x + 1$	$\zeta_{12} + \zeta_{12}^2$	$2 + 2\zeta_{12} - \zeta_{12}^3$	ζ_{12}^3
7	$x^3 - 5x^2 + 6x - 1$	$-\zeta_7 - \zeta_7^3$	$2 + \zeta_7^2 + \zeta_7^5$	ζ_7^4
7	$x^3 - 6x^2 + 5x - 1$	$-\zeta_7 - \zeta_7^2 - \zeta_7^5$	$2 - \zeta_7^2 + \zeta_7^3 + \zeta_7^4 - \zeta_7^5$	ζ_7^3
30	$x^4 - 7x^3 + 14x^2 - 8x + 1$	$-\zeta_{30}^6 + \zeta_{30}^8$	$1 - \zeta_{30} - \zeta_{30}^2 + \zeta_{30}^4 + \zeta_{30}^5 - \zeta_{30}^7$	ζ_{30}^{-1}
30	$x^4 - 8x^3 + 14x^2 - 7x + 1$	$\zeta_{30}^2 - \zeta_{30}^6 + \zeta_{30}^{14}$	$4 - \zeta_{30}^2 - 2\zeta_{30}^3 - 2\zeta_{30}^4 - \zeta_{30}^5 + \zeta_{30}^6 + 3\zeta_{30}^7$	ζ_{30}^7

Table 1: Minimal polynomials of α for some values of k in Lemma 3.11 for which γ is itself cyclotomic.

To prove (b), note that by [10], $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(k)$ if $k \notin \{7, 30\}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(k)/2$ if $k \in \{7, 30\}$. This confirms the claimed value of $\deg(S(x))$. To read off the mod-2 reduction, we use [2, (4.0.1)]: $Q(x)$ is either equal (for $k \notin \{7, 30\}$) or a factor (for $k \in \{7, 30\}$) of

$$\prod_{\substack{0 \leq i \leq k/2 \\ \gcd(k,i)=1}} (x^2 - (4 + 2 \cos \frac{2\pi i}{n})x + 1) \equiv \prod_{\substack{0 \leq i \leq k/2 \\ \gcd(k,i)=1}} (x^2 - (\frac{2\pi i}{n})x + 1) \equiv \Phi_k(x) \pmod{2}.$$

□

Remark 3.12. Let $\{P_n(x)\}_{n \geq 0}$ be a sequence of monic integer polynomials satisfying (3.1), and let α be an algebraic integer which is *not* a unit. Then Lemma 3.10 implies that the set of nonnegative integers n such that $P_n(\alpha) = 0$ contains at most one element. One can further say that this set can always be determined explicitly; this amounts to the fact that the *Skolem problem* is solved for second-order linear recurrences (although not for recurrences of arbitrary order).

4 Some auxiliary polynomials

We next follow [3, § 3] and create a family of sequences of polynomials satisfying (3.1). There is again an adjustment of indexing relative to [3].

Define the element

$$g_{n,k}(x) := x^{-k}(w^n(w+1)^k + (x-w-1)^n(x-w)^k) \in R, \quad (4.1)$$

so in particular $g_{n,0}(x) = f_n(x)$. As in [3, Lemma 3.11], we have the following (but with a different proof).

Lemma 4.2. *For $n \geq k \geq 0$, $g_{n,k}(x)$ is a monic polynomial over $\mathbb{Z}$ of degree n .*

Proof. We give two different derivations, each of which provides some useful extra information. First, since $g_{n,k}(x)$ is invariant under the automorphism $w \mapsto x - w - 1$ of $\mathbb{Q}(x)[w]/(w^2 - (x-1)w + x)$, we have $g_{n,k}(x) \in \mathbb{Q}(x)$. By rewriting the defining relation of R as $w(w+1) = x(w-1)$, we obtain

$$g_{n,k}(x) = w^{n-k}(w-1)^k + (x-w-1)^{n-k}(x-w-2)^k; \quad (4.3)$$

since w is integral over $\mathbb{Z}[x]$, so is $g_{n,k}(x)$, and hence $g_{n,k}(x) \in \mathbb{Z}[x]$.

Second, by (3.6), we have $g_{n,0}(x) = f_n(x)$. More generally, by expanding in binomials, we have

$$g_{n,k}(x) = x^{-k} \sum_{i=0}^k \binom{k}{i} f_{n+k-i}(x). \quad (4.4)$$

For $n \geq k$, we see from (2.2) and (4.4) that $x^k g_{n,k}(x)$ is a monic polynomial over $\mathbb{Z}$ of degree $n+k$. On the other hand, the relation $w^{-1}(w^2 - (x-1)w + x) = 0$ may be rewritten as

$$(x-1)(w+1) = x(w+w^{-1});$$

substituting into (4.1) and expanding again in binomials yields

$$g_{n,k}(x) = (x-1)^{-k} \sum_{i=0}^k \binom{k}{i} f_{n+k-2i}(x). \quad (4.5)$$

Combining (4.1) and (4.5), we deduce that for $n \geq k$,

$$g_{n,k}(x) \in \mathbb{Z}[x^\pm] \cap \mathbb{Z}[(x-1)^\pm] = \mathbb{Z}[x]$$

as claimed. $\square$

Combining (4.5) with (2.7) and (2.9) respectively, we obtain evaluations at special points:

$$g_{n,k}(0) = (-1)^n 2^k \quad (n > k) \quad (4.6)$$

$$g_{n,k}(3 \pm 2\sqrt{2}) = 2(\pm\sqrt{2})^k (1 \pm \sqrt{2})^{n-k} \quad (n \geq k). \quad (4.7)$$

Similarly, combining (4.5) with (2.11), we obtain the congruences

$$g_{n,k}(x) \equiv x^{n-k}(x+1)^k + 2^k \pmod{2} \quad (n > k) \quad (4.8)$$

$$g_{n,k}(x) \equiv x^{n-k}(x+1)^k + 2((n-k)x+n)x^{n-k}(x+1)^{k-2} \pmod{4} \quad (n > k \geq 2). \quad (4.9)$$

We also record the behavior of linear coefficients:

$$g_{n,k}(x) \equiv (-1)^n (2^k - (2n-k)2^k x) \pmod{x^2} \quad (n \geq k+2). \quad (4.10)$$

One can write down a number of additional recurrence relations satisfied by the $g_{n,k}$. For example, from (4.4) we have

$$xg_{n,k}(x) = g_{n+1,k-1}(x) + g_{n,k-1}(x). \quad (4.11)$$

From (4.4) and (2.6), we also have

$$g_{n,k}(x) - (x-1)g_{n-1,k}(x) + xg_{n-2,k}(x) = 0 \quad (n-2 \geq k \geq 0); \quad (4.12)$$

that is, for fixed k , for $n \geq k$ we again get a sequence of polynomials satisfying (3.1). As in [3, Lemma 3.8], we can derive some additional recurrences such as

$$g_{n+1,k}(x) - g_{n+1,k-1}(x) + g_{n,k-1}(x) = 0 \quad (n \geq k \geq 1) \quad (4.13)$$

$$g_{n,k}(x) - (x-3)g_{n-1,k-1}(x) + 2g_{n-2,k-2}(x) = 0 \quad (n \geq k \geq 2) \quad (4.14)$$

$$g_{n+2,k}(x) + 4g_{n+1,k-1}(x) + 4g_{n,k-2}(x) - x^2g_{n,k}(x) = 0 \quad (n \geq k \geq 2) \quad (4.15)$$

by the following process:

- Check the identity when k is as small as possible (i.e., $k = 1$ for (4.13); $k = 2$ for (4.14), (4.15)) and $n \in \{k, k+1\}$.
- Using (4.12), deduce by induction on n that the claim holds whenever k is as small as possible and $n \geq k$.
- Using (4.11), deduce by induction on k that the claim holds for all allowed n and k .

5 Sequences of polynomials with real roots

We next prove a close analogue of [3, Lemma 4.1] in order to generate a number of sequences of polynomials satisfying (3.1) and having all roots in the interval $[a, b]$. In the process, we extract some extra information in order to compare this construction with a more flexible construction to follow (Theorem 6.2).

For A and B two polynomials over $\mathbb{R}$, we say that B *interlaces* A if:

- $\deg(A) = \deg(B) + 1$;
- all of the complex roots of A and B are real;
- and the roots of A and B weakly alternate, that is, the roots of A can be labeled $\alpha_1, \dots, \alpha_d$ and the roots of B can be labeled $\beta_1, \dots, \beta_{d-1}$ in such a way that

$$\alpha_1 \leq \beta_1 \leq \alpha_2 \leq \dots \leq \alpha_{d-1} \leq \beta_{d-1} \leq \alpha_d.$$

Lemma 5.1. *Let $a_0, \dots, a_k$ be a sequence of real numbers with $a_k = 1$, such that the polynomial $Q(z) := \sum_{i=0}^k a_i z^i$ has all of its complex roots inside the open disc $|z| < \sqrt{2}$. Then for each $n \geq k$, the roots of the polynomial*

$$P_n(x) := \sum_{i=0}^k a_i g_{n-k+i,i}(x) \quad (5.2)$$

are all real, simple, and contained in $[a, b]$. Moreover, the roots of $P_{n+1}(x)$ and $P_n(x)$ are interlaced and

$$\frac{P_{n+1}(a)}{P_n(a)} = 1 - \sqrt{2}, \quad \frac{P_{n+1}(b)}{P_n(b)} = 1 + \sqrt{2}. \quad (5.3)$$

(Note that by (4.12), the sequence $\{P_n\}$ again satisfies (3.1); and by (4.6), $P_n(0) = (-1)^n Q(-2)$ for $n > k$.)

Proof. Define $x(\theta), y(\theta), s(\theta)$ as in the proof of [3, Lemma 4.1] and set $w(\theta) := e^{\pi i \theta} \sqrt{x(\theta)}$ (taking the positive square root of $x(\theta) > 0$). Now

$$P_n(x(\theta)) = \operatorname{Real} \left(2w(\theta)^{n-k} \sum_{i=0}^k a_i s(\theta)^i \right). \quad (5.4)$$

The zeroes of $P_n(x)$ in the interval $[a, b]$ (counted without multiplicity) are in bijection with zeros of $P_n(x(\theta))$ in either of the intervals $[-2\pi, 0]$ or $[0, 2\pi]$. We will estimate the number of zeros of $P_n(x(\theta))$ by computing the displacement of

$$\arg \left(w(\theta)^{n-k} \sum_{i=0}^k a_i s(\theta)^i \right) = (n-k) \arg w(\theta) + k \arg s(\theta) + \arg \left(\sum_{i=0}^k a_i s(\theta)^{i-k} \right)$$

over the interval $[-2\pi, 2\pi]$ (choosing all of the arguments to vary continuously in θ).

As θ varies from -2π to 2π , the displacement of $(n-k) \arg w(\theta) + k \arg s(\theta)$ equals $2n\pi$. Meanwhile, as in [3, Lemma 4.1], the condition on the roots of Q ensures that $\arg \left(\sum_{i=0}^k a_i s(\theta)^{i-k} \right)$ has displacement 0.

Since $\arg \left(w(\theta)^{n-k} \sum_{i=0}^k a_i s(\theta)^i \right)$ varies continuously from 0 to $2n\pi$ as θ runs from -2π to 2π , by the intermediate value theorem it evaluates to an odd multiple of π at no fewer than $2n$ distinct values in this range. By (5.4), these values are zeros of $P_n(x(\theta))$ in $[a, b]$, each counted at most twice. Since $P_n(x)$ is a polynomial of degree n , we deduce that all of its zeros are pairwise distinct real numbers in $[a, b]$; moreover, $\arg \left(w(\theta)^{n-k} \sum_{i=0}^k a_i s(\theta)^i \right)$ evaluates to an odd multiple of π at *exactly* $2n$ distinct values as θ runs from -2π to 2π .

We deduce (5.3) by applying (4.7) to obtain

$$P_n(3 \pm 2\sqrt{2}) = \sum_{i=0}^k 2a_i (\pm\sqrt{2})^i (1 \pm \sqrt{2})^{n-k} = 2(1 \pm \sqrt{2})^{n-k} Q(\pm\sqrt{2});$$

it thus remains to establish that the roots of $P_n(x)$ and $P_{n+1}(x)$ are interlaced. To wit, for $j \in \{1, \dots, n\}$, let $\theta_j \in [-2\pi, 0]$ be the unique value for which the displacement of $\arg \left(w(\theta)^{n-k} \sum_{i=0}^k a_i s(\theta)^i \right)$ over $[-2\pi, \theta_j]$ equals $(2j-1)\pi$, so that $x(\theta_j)$ is a root of $P_n(x)$. Now note that the displacement of

$$\arg \left(w(\theta)^{n-k+1} \sum_{i=0}^k a_i s(\theta)^i \right) = \arg w(\theta) + \arg \left(w(\theta)^{n-k} \sum_{i=0}^k a_i s(\theta)^i \right)$$

over $[-2\pi, \theta_j]$ is strictly greater than $(2j-1)\pi$, so this function must reach an odd multiple of π no fewer than j times in this range. In other words, for every root r

of $P_n(x)$, there are more roots of $P_{n+1}(x)$ greater than r than there are roots of $P_n(x)$ greater than r . By an analogous argument, there are also more roots of $P_{n+1}(x)$ less than r than there are roots of $P_n(x)$ less than r . This implies that the roots of $P_n(x)$ and $P_{n+1}(x)$ are interlaced. $\square$

Remark 5.5. Note that expressing the sequence (5.2) in the form (3.5) using (4.3) yields

$$P_+ = w^{-k}Q(w-1), \quad P_- = (x-w-1)^{-k}Q(x-w-2).$$

The situation of Lemma 3.11 then implies that $(\gamma^2\alpha^{-1})^rQ(\gamma-1) + Q(\alpha-\gamma-2) = 0$ for some $r \in \{0, \dots, k-1\}$.

Remark 5.6. From (4.11), it follows at once that in Lemma 5.1, replacing the polynomial $Q(z)$ with $(z+1)Q(z)$ does not change the resulting sequence $\{P_n(x)\}$ except for the omission of the initial term $P_k(x)$. This means that it suffices to prove all of the assertions of Lemma 5.1 in the case $n = k$.

For example, the statement that the roots of $P_n(x)$ lie in $[a, b]$ (which implies [3, Lemma 4.1]) can be proved for $n = k$ as follows: use induction on n using (4.14) (plus (4.4) for the base case $n = 1$) to show that

$$(-x)^n g_{n,n}(3-x-2/x) = x^{2n} + 2^n; \quad (5.7)$$

use (5.7) to write

$$(-x)^k P_k(3-x-2/x) = \sum_{i=0}^k a_i (x^{2k-i} + 2^i x^i),$$

and then apply [1, Lemma 3.1]. This is not entirely surprising given that the proof of [3, Lemma 4.1] in the case $n = 0$ is functionally identical to the proof of [1, Lemma 3.1].

Remark 5.8. For any fixed positive integer m , Remark 5.6 implies that there are infinitely many monic integer polynomials $Q(z)$ with all roots in $|z| < \sqrt{2}$ such that $|Q(-2)| = m$. On the other hand, if we counteract Remark 5.6 by further requiring that $Q(-1) \neq 0$, then we only get finitely many such Q .

To see this, define the holomorphic function $f(z) = \frac{1+z}{2+z}$ on the disc $|z| \leq \sqrt{2}$. For $|z| = \sqrt{2}$, we have

$$|f(z)|^2 = \frac{1+z+\bar{z}+2}{4+2z+2\bar{z}+2} = \frac{1}{2};$$

by the maximum modulus principle, we deduce that $|f(z)| \leq 2^{-1/2}$ for all z in the disc. Now let $r_1, \dots, r_{\deg(Q)}$ denote the roots of Q and write

$$\frac{Q(-1)}{Q(-2)} = \prod_{i=1}^{\deg(Q)} f(r_i)$$

to deduce that $|Q(-1)| \leq |Q(-2)|2^{-\deg(Q)/2}$. If $Q(-1)$ is a nonzero integer, its absolute value is at least 1, and hence $|Q(-2)| \geq 2^{\deg(Q)/2}$; we conclude that fixing $|Q(-2)|$ imposes an upper bound on $\deg(Q)$. This in turn imposes a bound on the absolute value of each coefficient of Q (using the bound on the roots), and thus limits Q to a finite set.

Remark 5.9. For a fixed degree k , the transformation $Q(z) \rightarrow P_k(x)$ is invertible over $\mathbb{Q}$ but not over $\mathbb{Z}$: its image consists of those polynomials with $P_k(1) \equiv 0 \pmod{2}$.

6 More sequences of interlaced polynomials

We now describe a construction that significantly generalizes Lemma 5.1 by allowing a more flexible choice of initial conditions. This will help us handle some cases where we do not have enough flexibility to choose the polynomial $Q(z)$ because of Remark 5.8.

Lemma 6.1. *Let $P_{n-1}(x), P_{n-2}(x)$ be polynomials over $\mathbb{R}$ satisfying the following conditions for some integer $d > 1$.*

- (i) *The polynomial P_{n-2} has degree $d - 2$ and has positive leading coefficient, and the polynomial P_{n-1} is monic of degree $d - 1$.*
- (ii) *The complex roots of P_{n-1} and P_{n-2} are all simple and contained in (a, b) .*
- (iii) *The polynomial P_{n-2} interlaces P_{n-1} . (This condition should be regarded as vacuously true when P_{n-2} is constant.)*
- (iv) *We have*

$$\frac{P_{n-1}(a)}{P_{n-2}(a)} \leq 1 - \sqrt{2}, \quad \frac{P_{n-1}(b)}{P_{n-2}(b)} \geq 1 + \sqrt{2}.$$

Then the polynomial $P_n(x)$ characterized by (3.1) has the following properties.

- (a) *The polynomial P_n is monic of degree d .*
- (b) *The complex roots of P_n are all simple and contained in (a, b) .*
- (c) *The polynomial P_{n-1} interlaces P_n .*
- (d) *We have*

$$\frac{P_n(a)}{P_{n-1}(a)} \leq 1 - \sqrt{2}, \quad \frac{P_n(b)}{P_{n-1}(b)} \geq 1 + \sqrt{2}.$$

Proof. As this result may be of more general interest, we have given a more general formulation in an appendix (Theorem A.3). Specializing that result by taking $A = 1, B = -1, C = -1, D = 0, y = 3 - 2\sqrt{2}, z = 3 + 2\sqrt{2}$ and computing that $\alpha = 1 - \sqrt{2}, \beta = 1 + \sqrt{2}$ yields the stated result. $\square$

Theorem 6.2. *Let P_0, P_1 be polynomials over $\mathbb{R}$ satisfying the following conditions.*

- (i) *The polynomial P_1 is monic, the polynomial P_0 has positive leading coefficient, and $\deg(P_1) = \deg(P_0) + 1$.*
- (ii) *The complex roots of P_0 and P_1 are all simple and contained in (a, b) .*

(iii) The polynomial P_0 interlaces P_1 . (This condition should be regarded as vacuously true when P_0 is constant.)

(iv) We have

$$\frac{P_1(a)}{P_0(a)} \leq 1 - \sqrt{2}, \quad \frac{P_1(b)}{P_0(b)} \geq 1 + \sqrt{2}.$$

Define the polynomials $P_n(x)$ for $n \geq 2$ so that (3.1) holds. Then for $n \geq 1$, P_n is monic of degree $\deg(P_0) + n$; the complex roots of P_n are all simple and contained in (a, b) ; and P_{n-1} interlaces P_n .

Proof. This follows from Lemma 6.1 by induction. $\square$

Remark 6.3. Any sequence as in Lemma 5.1 satisfies the hypotheses and conclusions of Theorem 6.2. In fact, it should be possible to deduce Lemma 5.1 entirely from Theorem 6.2, but we did not work this out.

Remark 6.4. Notably, (3.1) implies that P_n is monic and $(-1)^n P_n(0)$ is constant for $n = 1, 2, \dots$ but *not* for $n = 0$. This gives us a fair bit of flexibility: given a monic integer polynomial P_1 whose complex roots are simple and contained in (a, b) , if we can find another integer polynomial P_0 satisfying the conditions of Theorem 6.2, then the sequence $P_1, P_2, \dots$ corresponds to a sequence of isogeny classes of abelian varieties over $\mathbb{F}_2$ of fixed order.

One key case where conditions (i)–(iii) of Theorem 6.2 all hold easily is when P_1 is monic and P_0 is its derivative. Unfortunately, this case is not directly useful because condition (iv) translates into a rather strong restriction: if we label the roots as $\alpha_1, \dots, \alpha_d$, then we must have

$$\sum_{i=1}^d \frac{1}{\alpha_i - a} \leq \sqrt{2} + 1, \quad \sum_{i=1}^d \frac{1}{b - \alpha_i} \leq \sqrt{2} - 1.$$

In particular,

$$2\sqrt{2} \geq \sum_{i=1}^d \left(\frac{1}{\alpha_i - a} + \frac{1}{b - \alpha_i} \right) \geq \frac{4d}{b - a}$$

and hence $d \leq 4$.

One may interpret the difficulty here as being caused by the fact that P'_1 has the rather large leading coefficient d . If one can instead find a integer polynomial P_0 of the same degree with a smaller leading coefficient whose roots also interlace those of P_1 , then one may have a better chance to satisfy condition (iv). In practice, we will present cases where P_0 is also monic.

7 Even orders: small cases

We next resolve Conjecture 1.2 in some cases where m is even, using Theorem 6.2 and some analysis of 2-adic Newton polygons. We start with the case $m = 2$ where the situation is easiest to explain.

Theorem 7.1. *For every positive integer g , there exists a simple abelian variety A of dimension g over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = 2$. In particular, Conjecture 1.2 holds for $m = 2$.*

Proof. The polynomials

$$P_0(x) = 1, \quad P_1(x) = x - 2$$

satisfy the hypotheses of Theorem 6.2 (treating (ii) as vacuously true in this setting). For $n \geq 1$, the resulting polynomial P_n is monic of degree n with constant term $(-1)^n 2$ and the complex roots of P_n all lie in $[a, b]$. Moreover, $P_n(x) \equiv x^n \pmod{2}$, so P_n is irreducible over $\mathbb{Q}_2$ (by the Schönemann–Eisenstein criterion: the Newton polygon has no interior vertices) and hence over $\mathbb{Q}$. Applying Lemma 2.1 yields the desired sequence of abelian varieties. $\square$

To extend this strategy to other even m , it is useful to allow some additional flexibility in the 2-adic Newton polygon. The following special case both exhibits a key idea of the general argument for m even (Theorem 10.5) and covers a special case that is missed by the general argument.

Theorem 7.2. *Conjecture 1.2 holds for $m = 20$.*

Proof. The polynomials

$$P_0(x) = x^3 - 10x^2 + 29x - 24, \quad P_1(x) = x^4 - 12x^3 + 47x^2 - 66x + 20$$

satisfy the hypotheses of Theorem 6.2. We have

$$P_n(x) \equiv x^{n+3} + x^{n+1} \pmod{2}, \quad P_n(x) \equiv 2x \pmod{4, x^2}.$$

Hence the 2-adic Newton polygon of P_n has slopes 0 with multiplicity 2, $1/n$ with multiplicity n , and 1 with multiplicity 1. In particular, for $n > 1$, the slope $1/n$ corresponds to an irreducible factor of P_n over $\mathbb{Q}_2$; consequently, if P_n is reducible over $\mathbb{Q}$, then it admits an irreducible factor S with $\deg(S) \leq 3$. By Lemma 3.10, this can only occur finitely often with $|S(0)| > 1$. If $|S(0)| = 1$, then $\deg(S) \leq 2$; we may then apply Lemma 3.11, noting that $k \in \{1, 2, 3, 4, 6\}$, then compute $P_n(x)$ for $n \leq 6$ and check that no such factor S occurs. $\square$

Remark 7.3. As written, Theorem 7.2 does not specify an explicit constant g_0 such that for every positive integer $g \geq g_0$, there exists a simple abelian variety A of dimension g over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = 20$. However, one can obtain such a constant from the proof: compute the finite list of monic irreducible polynomials S with $\deg(S) \leq 3$ and $S(0) \in \{2, 4, 5, 10, 20\}$ having all roots in $[a, b]$, then apply Remark 3.12 to the roots of these polynomials. Similar considerations will apply to the other results feeding into Theorem 1.3.

8 Odd prime orders: small cases

We now resolve Conjecture 1.2 in some cases where m is an odd prime, again using Theorem 6.2. In this case the 2-adic Newton polygon is of no help, so we instead use the mod-2 reduction to narrow the possibilities for a recurrent polynomial factor of order 1.

Lemma 8.1. *With notation as in Lemma 3.11, suppose that $x^d + 1 \in \mathbb{Z}[x]$ belongs to the ideal $(2, S(x))$. Then k divides $2d$.*

Proof. Suppose first that $k \notin \{7, 30\}$. Then $S(x) \equiv \Phi_k(x) \pmod{2}$, so the evaluation of $x^d + 1$ at a primitive k^{th} root of unity ζ_k is divisible by 2 in the ring of cyclotomic integers. By [5, Theorem 6.7, Corollary 6.8], this is only possible if $\zeta_k^d = \pm 1$, which yields (a).

Now suppose $k \in \{7, 30\}$. Then $\Phi_k(x)$ splits modulo 2 as a product of two factors which are reciprocals of each other, and $S(x)$ is congruent to one of these; however, since $x^d + 1$ is itself reciprocal, $(x^d + 1) \pmod{2}$ is divisible by both factors and the preceding logic applies. $\square$

Theorem 8.2. *For every positive integer g , there exists a simple abelian variety A of dimension g over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = 3$. In particular, Conjecture 1.2 holds for $m = 3$.*

Proof. The polynomials

$$P_0(x) = 1, \quad P_1(x) = x - 3$$

satisfy the hypotheses of Theorem 6.2 (treating (ii) as vacuously true in this setting). We compute that

$$P_n(x) \equiv x^n + x^{n-1} + \cdots + 1 = \frac{x^{n+1} - 1}{x - 1} \pmod{2}.$$

Suppose that P_n is reducible for some $n > 0$; since $|P_n(0)| = 3$ is prime, P_n must then admit an irreducible factor S with $S(0) = \pm 1$. We may thus set notation as in Lemma 3.11.

For $P_n(x)$ to be divisible by $S(x)$ in $\mathbb{F}_2[x]$, by Lemma 8.1 we must have either $k|(n+1)$; or $2|k$, $(k/2)|(n+1)$, and $r = k/2$. In the first case, combining with Lemma 3.11(a), we see that $P_{n'}(\alpha) = 0$ whenever $n' \equiv k-1 \pmod{k}$; running the recurrence (3.1) backwards, we deduce that α is a root of $P_{-1}(x) = -\frac{2}{x}$, a contradiction. In the second case, writing P_n in the form (3.5), we have $P_+\gamma^{-1} = P_-(\alpha - 1 - \gamma)^{-1} = \frac{1}{2}P_{-1}(\alpha)$; hence

$$P_0(\alpha) = (P_+\gamma^{-1})\gamma + (P_-(\alpha - 1 - \gamma))^{-1}(\alpha - 1 - \gamma) = \frac{1}{2}(\alpha - 1)P_{-1}(\alpha),$$

which is to say that α is a root of $(x-1)P_{-1}(x) - 2P_0(x) = -\frac{2}{x}$, another contradiction.

We conclude that P_n is irreducible for all $n > 0$; applying Lemma 2.1 yields the desired sequence of abelian varieties. $\square$

Remark 8.3. In principle, the same approach can be applied whenever m is an odd prime, contingent on the identification of a suitable sequence. To illustrate a complication that can arise, we consider a failed example of this approach for $m = 7$: the polynomials

$$P_0(x) = x^3 - 9x^2 + 21x - 5, \quad P_1(x) = x^4 - 11x^3 + 37x^2 - 37x + 7$$

satisfy the hypotheses of Theorem 6.2, and the resulting sequence has the desired mod-2 structure, but $P_{-1}(x)$ is divisible by $x^2 - 4x + 1$ and $P_0(x)$ is divisible by $x^2 - 5x + 1$. By Lemma 3.11, it follows that infinitely many of the P_n are divisible by $x^2 - 4x + 1$ or $x^2 - 5x + 1$; correspondingly, the proof of Theorem 8.2 breaks down because $P_{-4}(x)$ is divisible by $x^2 - 4x + 1$ and $(x-1)P_{-4}(x) - 2P_{-3}(x)$ is divisible by $x^2 - 5x + 1$.

m	$P_0(x)$	$P_1(x)$	$P_n(x) \pmod{2}$
5	$x - 2$	$x^2 - 5x + 5$	$x^{n+1} + x^n + 1$
11	$x^2 - 7x + 8$	$x^3 - 9x^2 + 21x - 11$	$x^{n+2} + x^{n+1} + x^n + 1$
13	$x^2 - 7x + 9$	$x^3 - 9x^2 + 22x - 13$	$x^{n+2} + x^{n+1} + 1$
19	$x^2 - 7x + 11$	$x^3 - 9x^2 + 24x - 19$	$x^{n+2} + x^{n+1} + 1$

Table 2: Polynomials used in the proof of Theorem 8.6.

To make the previous construction more flexible, we analyze some other possible mod-2 reductions.

Lemma 8.4. *With notation as in Lemma 3.11, suppose that $x^d + x^e + 1 \in \mathbb{Z}[x]$ belongs to the ideal $(2, S(x))$. Assume also that $k \notin \{7, 30\}$. Then 3 divides k and $k/3$ divides $2 \gcd(d, e)$.*

Proof. By applying [5, Theorem 6.7, Corollary 6.8] as in the proof of Lemma 8.1, we see that $\pm \zeta_k^d$ and $\pm \zeta_k^e$ must be distinct primitive third roots of unity. This proves all of the claims. $\square$

Lemma 8.5. *With notation as in Lemma 3.11, suppose that $x^d + x^e + x^f + 1 \in \mathbb{Z}[x]$ belongs to the ideal $(2, S(x))$. Assume also that $k \notin \{7, 30\}$. Then there exists a permutation c_1, c_2, c_3 of $\{d, e, f\}$ such that k divides $2 \gcd(c_1, c_2 - c_3)$.*

Proof. By applying [5, Theorem 6.7, Corollary 6.8] as in the proof of Lemma 8.1, we see that for some choice of signs, $\pm \zeta_k^d, \pm \zeta_k^e, \pm \zeta_k^f, 1$ must cancel in pairs. This proves the claim. $\square$

Theorem 8.6. *Conjecture 1.2 holds for $m = 5, 11, 13, 19$.*

Proof. For each listed m , we identify a sequence generated by Theorem 6.2 with the property that $|P_1(0)| = m$; see Table 2 for the list of polynomials used and the mod-2 reduction of $P_n(x)$. Since $|P_n(0)| = m$ is prime, if P_n is reducible, then it admits an irreducible factor S with $S(0) = \pm 1$, and we may set notation as in Lemma 3.11. Reducing modulo 2 and applying Lemma 8.4 (if $m \in \{5, 13, 19\}$) or Lemma 8.5 (if $m = 11$) we see that necessarily $k \leq 30$; we may rule this out by checking that P_n is irreducible for $n = 0, \dots, 29$ and then applying Lemma 3.11(a).

We conclude that P_n is irreducible for all $n > 0$; applying Lemma 2.1 yields the desired sequence of abelian varieties. $\square$

Remark 8.7. In the proof of Theorem 8.6, allowing all $k \leq 30$ is overkill: when $P_n(x)$ reduces to a trinomial we must have $k \in \{3, 6, 7, 30\}$, while when $P_n(x)$ reduces to a tetranomial we must have $k \in \{2, 4, 7, 30\}$.

9 Prime power orders: small cases

We next combine ideas from the previous arguments to cover some higher prime powers; this will in particular cover some even integers missed by the general construction in Theorem 10.5 and some odd integers missed by the general construction in Theorem 12.5.

Theorem 9.1. *Conjecture 1.2 holds for $m = 4, 8$.*

Proof. For each listed m , we identify a sequence generated by Theorem 6.2 with the property that $|P_1(0)| = m$; see Table 3 for the list of polynomials used and the mod-2 reduction of $P_n(x)$. From the latter, we see that the 2-adic Newton polygon of P_n has a single nonzero slope with multiplicity 1; consequently, P_n cannot factor as a product of two polynomials with constant terms of absolute value greater than 1. That is, if P_n is reducible, then it admits an irreducible factor S with $S(0) = \pm 1$, and we may set notation as in Lemma 3.11. Applying Lemma 8.5, we see that necessarily $k \leq 30$; we may rule this out by checking that P_n is irreducible for $n = 0, \dots, 29$ and then applying Lemma 3.11(a).

We conclude that P_n is irreducible for all $n > 1$; applying Lemma 2.1 yields the desired sequence of abelian varieties. $\square$

Corollary 9.2. *For $m \in \{2, 3, 4, 5\}$, for every positive integer g , there exists a simple abelian variety A of dimension g over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = m$.*

Proof. For $m = 2$ and $m = 3$, this is the statements of Theorem 7.1 and Theorem 8.2 respectively. For $m = 4$, the proof of Theorem 9.1 implies this for $g \geq 3$; we may add $g = 1, 2$ by direct inspection. For $m = 5$, the proof of Theorem 8.6 implies the claim for $g \geq 2$; we may add $g = 1$ by direct inspection. $\square$

Theorem 9.3. *Conjecture 1.2 holds for $m = 9, 25, 27, 49, 81$.*

Proof. For each listed m , we identify a sequence generated by Theorem 6.2 with the property that $|P_1(0)| = m$; see Table 3 for the list of polynomials used, the mod-2 reduction of $P_n(x)$ and the value of c for which for $n > 1$,

$$P_n(x) \equiv (-1)^{\deg(P_n)-1}((2mn + c)x - m) \pmod{x^2}.$$

Let p be the unique prime divisor of m . Since $c \not\equiv 0 \pmod{p}$, the p -adic Newton polygon has the unique nonzero slope $\log_p(m)$ with multiplicity 1. Consequently, P_n cannot factor as a product of two polynomials with constant terms of absolute value greater than 1; that is, if P_n is reducible, then it admits an irreducible factor S with $S(0) = \pm 1$, and we may set notation as in Lemma 3.11. Applying Lemma 8.4 or Lemma 8.5, we see that necessarily $k \leq 30$; we may rule this out by checking that P_n is irreducible for $n = 0, \dots, 29$ and then applying Lemma 3.11(a).

We conclude that P_n is irreducible for all $n > 1$; applying Lemma 2.1 yields the desired sequence of abelian varieties. $\square$

m	$P_0(x)$	$P_1(x)$	$P_n(x) \pmod{2}$	c
4	$x^2 - 6x + 3$	$x^3 - 9x^2 + 20x - 4$	$x^{n+2} + x^{n+1} + x^n + x$	
8	$x - 3$	$x^2 - 6x + 8$	$\frac{x^{n+2} + x^{n+1} + x^n + x}{x+1}$	
9	$x^2 - 6x + 6$	$x^3 - 8x^2 + 17x - 9$	$x^{n+2} + x^n + 1$	-4
25	$x^3 - 10x^2 + 28x - 18$	$x^4 - 12x^3 + 46x^2 - 61x + 25$	$x^{n+3} + x^n + 1$	4
27	$x^3 - 10x^2 + 29x - 21$	$x^4 - 12x^3 + 48x^2 - 71x + 27$	$x^{n+3} + x + 1$	11
49	$x^3 - 11x^2 + 37x - 38$	$x^4 - 13x^3 + 57x^2 - 96x + 49$	$\frac{x^{n+4} + x^{n+1} + x^n + 1}{x+1}$	-13
81	$x^4 - 12x^3 + 51x^2 - 90x + 55$	$x^5 - 14x^4 + 73x^3 - 176x^2 + 196x - 81$	$x^{n+4} + x^{n+2} + 1$	8

Table 3: Polynomials used in the proofs of Theorem 9.1 and Theorem 9.3.

Remark 9.4. To see what happens if we fail to control the linear coefficient in the setting of Theorem 9.3, consider the sequence with

$$P_0(x) = x^2 - 7x + 11, \quad P_1(x) = x^3 - 9x^2 + 22x - 9.$$

For $n > 1$,

$$P_n(x) \equiv (-1)^{n-1}((18n+6)x - 9) \pmod{x^2}.$$

We thus cannot rule out factorizations such as

$$P_3(x) = (x^2 - 5x + 3)(x^3 - 8x^2 + 15x - 3).$$

10 Even orders: large cases

We now prove Conjecture 1.2 in all remaining cases where m is even. This involves combining the use of 2-adic Newton polygons as in §7 (especially the proof of Theorem 7.2) with the construction of convenient polynomials for Lemma 5.1 using the techniques of [3, § 8].

For m a positive integer, we say that a monic integer polynomial $Q(z)$ is a *compliant representation* of m if the following conditions hold:

- $Q(2) = m$;
- $Q(z) \equiv (z-1)^{\deg(Q)-c} z^c \pmod{2}$, where $c = 0$ if m is odd and $c = 1$ if m is even;
- $Q(z)$ has all complex roots in the disc $|z| < \sqrt{2}$.

For m odd, this reproduces the definition of [3, § 8]. If m_1 is odd, m_2 is even, and $Q_i(z)$ is a compliant representation of m_i , then $(Q_1 Q_2)(z)$ is a compliant representation of $m_1 m_2$.

Lemma 10.1. *For any even positive integer m , if m admits a compliant representation, then Conjecture 1.2 holds for m .*

Proof. Let $Q(-z)$ be a compliant representation of m (noting the substitution $z \mapsto -z$); we may assume without loss of generality that Q is not divisible by $z + 1$. Define the polynomials $P_n(x)$ as in Lemma 5.1. It suffices to prove that P_n is irreducible for all but finitely many n , as then we may apply Lemma 2.1 to conclude.

By (4.6) and (5.2), we have $P_n(0) = (-1)^n Q(2) = (-1)^n m$, which in particular is even. By (4.8) and (5.2), for $n > k$ we have

$$P_n(x) \equiv \sum_{i=0}^k a_i x^{n-k}(x+1)^i \equiv x^{n-k} Q(x+1) \equiv x^n + x^{n-1} \pmod{2}.$$

If $m \equiv 2 \pmod{4}$, we deduce at once that the 2-adic Newton polygon of P_n consists of the slopes 0 with multiplicity 1 and $1/(n-1)$ with multiplicity $n-1$.

If $m \equiv 0 \pmod{4}$, we need to compute modulo 4. From (2.11) and (4.5), we see that for $n \gg 0$,

$$\begin{aligned} g_{n-k,0}(x) &\equiv 2(n-k)x + 1 \pmod{4, x^2} \\ g_{n-k+1,1}(x) &\equiv 2x \pmod{4, x^2} \\ g_{n-k+i,i}(x) &\equiv 0 \pmod{4, x^2} \quad (i \geq 2). \end{aligned}$$

Since $Q(0) = m$ is even, we deduce that the coefficient of x in P_n is congruent to 2 modulo 4 for $n \gg 0$. We deduce that the 2-adic Newton polygon of P_n consists of the slopes 0 with multiplicity 1, $1/(n-2)$ with multiplicity $n-2$, and $v_2(m) - 1$ with multiplicity 1.

In either case, we see that over $\mathbb{Q}_2$, P_n admits an irreducible factor of degree at least $n-2$; consequently, if P_n is reducible over $\mathbb{Q}$, it admits an irreducible factor R of degree at most 2. By Lemma 3.10, there can be only finitely many such cases where this factor satisfies $|R(0)| > 1$.

If $|R(0)| = 1$, then returning to the Newton polygon shows that in fact $\deg(R) \leq 1$. This leaves only the possibility that $R(x) = x - 1$; however, from (2.8) and the fact that $Q(0)$ is even, we deduce that $P_n(1) \equiv 2 \pmod{4}$ for $n \gg 0$, so this case is also excluded. $\square$

In order to apply the techniques of [3, § 8] to construct compliant representations, we must first correct some errors in the numerics given in [3, Lemma 8.5]; we also record an additional observation that will be used later. For any polynomial $Q(z)$ with all complex roots in the disc $|z| < \sqrt{2}$, define the *quality* of Q as in [3, (8.4)]:

$$\text{qual}(Q(z)) := \min\{|Q(z)| : |z| \geq \sqrt{2}\}.$$

By the maximum modulus principle, the minimum is achieved on the circle $|z| = \sqrt{2}$.

Lemma 10.2. *Let m be an odd positive integer.*

- (a) Any $m \in (0, 512)$ admits a compliant representation.
- (b) Any $m \in (512, 5166)$ admits a compliant representation of quality at least $\frac{10}{7} > \sqrt{2}$.
- (c) Any $m \in (5166, 9414)$ admits a compliant representation of quality at least $\frac{55}{7} > 7$.
- (d) Any $m \in (9414, 32400)$ admits a compliant representation of quality at least 11.
- (e) Any $m \in (32402, 142000)$ admits a compliant representation of quality at least $\frac{132}{7}$.

Proof. We first run an exhaust over monic polynomials Q of degree at most 9 (rather than 7 as in *loc. cit.*), with all coefficients in $\{-3, \dots, 3\}$ and $m = Q(0)$ odd, checking whether Q is a compliant representation of m . For each value of m that is successfully represented at least once, we record the compliant representation with the maximum observed quality, rounding the latter down to the nearest multiple of $\frac{1}{7}$.

We then compute, for each odd integer $m \in \{1, 142000\}$, a lower bound on the maximum quality of a compliant representation of m using the logic used in the proof of [3, Lemma 8.5]. For this, we must correct an error in the code in [3, Appendix]: the lines

```
q = (rep_quality[m1]*rep_quality[m2])/7 - abs(c)
if m not in rep_quality or rep_quality[m] < q:
```

should instead read

```
q = (rep_quality[m1]*rep_quality[m2])/7 - 7*abs(c)
if q > 0 and (m not in rep_quality or rep_quality[m] < q):
```

From the results of this computation, we read off (a)–(e). □

This in turn yields a corrected proof of [3, Lemma 8.7].

Lemma 10.3. *Every odd positive integer admits a compliant representation.*

Proof. By Lemma 10.2(a,b), it suffices to check that for $m \geq 5167$ odd, each of $\{m, m+2, \dots, 15m-16\}$ admits a representation with quality at least 7. The base case $m = 5167$ holds by Lemma 10.2(c–e) because $15 \cdot 5167 - 16 < 142000$; the proof of the induction step is unchanged from [3, Lemma 8.7]. □

Lemma 10.4. *Let m be an even positive integer.*

- (a) If $m \equiv 2 \pmod{4}$, then m admits a compliant representation.
- (b) If $m \equiv 0 \pmod{4}$ and $m \notin \{4, 8, 20\}$, then m admits a compliant representation.

Proof. By Lemma 10.3, every odd positive integer m admits a compliant representation $Q(z)$, and then $zQ(z)$ is a compliant representation of $2m$. This yields (a).

By Lemma 10.2 and Lemma 10.3, every odd integer $m \geq 513$ admits a compliant representation $Q(z)$ of quality at least $\frac{10}{7} > \sqrt{2}$. For such m and Q , $zQ(z) - 2$ is a compliant representation of $2m - 2$; this yields a compliant representation of every $m \equiv 0 \pmod{4}$ with $m \geq 1024$.

To close the range, we adapt the proof of Lemma 10.2 as follows. We first run an exhaust over monic polynomials Q of degree at most 9 with all coefficients in $\{-3, \dots, 3\}$ and $m = Q(0)$ even, checking whether Q is a compliant representation of m . We then combine with the result of the computation proving Lemma 10.2, then look for additional compliant representations using the following logic: if Q_1 is a compliant representation of an integer $m_1 \equiv 0 \pmod{4}$ of quality q_1 , Q_2 is a compliant representation of an odd integer m_2 of quality q_2 , and $c \equiv 0 \pmod{4}$ is an integer with $q_1 q_2 > |c|$, then $R(z) = Q_1(z)Q_2(z) + c$ is a compliant representation of $m_1 m_2 + c$ of quality at least $q_1 q_2 - |c|$. This computation yields compliant representations of all $m \equiv 0 \pmod{4}$ with $4 \leq m \leq 1024$ and $m \notin \{4, 8, 20\}$. $\square$

Combining Lemma 10.1 with Lemma 10.4 yields the following result.

Theorem 10.5. *Conjecture 1.2 holds for every positive even integer $m \notin \{4, 8, 20\}$.*

11 Odd prime orders: large cases

We now prove Conjecture 1.2 in all remaining cases where m is an odd prime less than 100, by modifying the construction used for even integers. We first extract some more information from the proof of Lemma 10.3.

Lemma 11.1. *For every $K > 0$, there exists some $m_0 > 0$ depending on K such that every odd positive integer $m \geq m_0$ admits a compliant representation of quality at least K . In particular:*

- (a) *for $K = 11$ we may take $m_0 = 9414$;*
- (b) *for $K = \frac{132}{7}$ we may take $m_0 = 32403$;*
- (c) *for $K = \frac{296}{7}$ we may take $m_0 = 486031$;*
- (d) *given a value of m_0 that works for some K , the value $15m_0 - 14$ works for $3K - 14$.*

Proof. We repeat the key argument from the proof of Lemma 10.3. Say we are given some odd m and some $K \geq 7$ such that each of $\{m, m+2, \dots, 15m-16\}$ admits a compliant representation with quality at least K . Then for n in this range, for c an even integer with $|c| \leq 14$, for any compliant representation $Q(z)$ of n of quality at least K , $(z^4 - 1)Q(z) + c$ is a compliant representation of $15m + c$ of quality at least $3K - 14$. This in particular implies (d), which in turn implies the first assertion.

To deduce (a), note that Lemma 10.2(d–e) verifies the claim for $m_0 \leq m \leq 142000$. Since $15 \cdot 9414 - 14 < 142000$, we may repeatedly apply the previous paragraph to conclude.

To deduce (b), note that Lemma 10.2(e) again verifies the claim for $m_0 \leq m \leq 142000$. Combining (a) with the first paragraph, and using the fact that $3 \cdot 11 - 14 > \frac{132}{7}$, we may extend the range to $m_0 \leq m \leq 15 \cdot 141999 - 14$; we may then repeatedly apply the first paragraph to conclude.

We deduce (c) by combining (b) and (d). $\square$

Remark 11.2. In case one needs to extend Lemma 11.1 for some reason, it is most efficient to use multiplication by an integer of the form $m = 2^{2^n} - 1$ which admits the compliant representation $Q(z) = z^{2^n} - 1$ of quality $2^{2^{n-1}} - 1 = \sqrt{m+1} - 1$. By increasing n , one can show that for any $\varepsilon > 0$, every sufficiently large m admits a compliant representation of quality at least $m^{1/2-\varepsilon}$.

For $R(z)$ a monic polynomial over $\mathbb{F}_2$, we say that a monic integer polynomial $Q(z)$ is an *R-compliant representation* of a positive integer m if the following conditions hold:

- $Q(2) = m$;
- $\deg(Q) \geq \deg(R)$ and $Q(z) \equiv (z-1)^{\deg(Q)-\deg(R)} R(z) \pmod{2}$;
- $Q(z)$ has all complex roots in the disc $|z| < \sqrt{2}$.

For example, our definition of compliant representations of even integers corresponds to the case $R(z) = z$. Hereafter, we restrict attention to odd m and take $R(z) := z^2 + z + 1$; this allows us to abstract some of our earlier arguments to prove Conjecture 1.2 for specific odd primes and prime powers.

Lemma 11.3. *Let $Q(-z)$ be an R-compliant representation of some odd positive integer m of degree d . Define the polynomials $P_n(x)$ as in Lemma 5.1. Suppose that for each row of Table 1, $P_n(\alpha) \neq 0$ for $n = d, \dots, d+k-1$. (For instance, this holds if $P_n(x)$ is irreducible for $n = d, \dots, d+29$.) If in addition m is prime, then Conjecture 1.2 holds for m .*

Proof. It suffices to prove that P_n is irreducible for all $n > d$, as then we may apply Lemma 2.1 to conclude. Since m is prime, if P_n is reducible, then it admits an irreducible factor with constant coefficient ± 1 , and we may set notation as in Lemma 3.11. Now note that for $n > d$,

$$P_n(x) \equiv x^n + x^{n-1} + x^{n-2} + 1 \pmod{2}. \quad (11.4)$$

Consequently, the situation in Lemma 8.5 can only arise for $k \leq 30$; per Remark 8.7, we only need to worry about $k \in \{2, 4, 7, 30\}$, and these cases are all ruled out by our hypothesis. $\square$

Remark 11.5. In Lemma 11.3, we can relax the hypotheses slightly. For $k = 2$, we need only check that $P_n(1) \neq 0$ for n even, as for n odd we may apply (2.8) to deduce that $P_n(1) \equiv 2 \pmod{4}$. For $k = 4$, we need only check that $P_n(\alpha) \neq 0$ for $n \in \{d, \dots, d+k-1\}$ with n odd. Similarly, for $k = 7$ we need only check $n \equiv 4, 5 \pmod{7}$, and for $k = 30$ we need only check $n \equiv 7, 10 \pmod{15}$. This means we only need to check the nonvanishing of 9 specific polynomial evaluations.

For an example where the hypothesis of Lemma 11.3 fails, note that for $Q(z) = z^2 - z + 1$, $P_4(x)$ is divisible by $x - 1$ and $P_5(x)$ is divisible by $x^3 - 5x^2 + 6x - 1$.

Lemma 11.6. *Let m be an odd (not necessarily prime) positive integer that admits an R-compliant representation $Q(z)$ of quality at least $\frac{239}{7}$. Then there exists an R-compliant representation of m to which the criterion of Lemma 11.3 applies.*

Proof. For $T(z) = z - 2$, we verify directly that $\max\{|T(z)| : |z| = \sqrt{2}\} = 2 + \sqrt{2}$ and that, if we define the sequence of polynomials $P_n(x)$ as in (5.2), then for each row of Table 1, $P_n(\alpha) \neq 0$ for $n = d, \dots, d + k - 1$. Since $10(2 + \sqrt{2}) < \frac{239}{7}$, the 11 distinct polynomials in the set

$$\{Q(z) + 2jT(z) : j = -5, \dots, 5\} \quad (11.7)$$

are all R -compliant representations of m , and at least one of them must satisfy the 9 nonvanishing conditions imposed in Remark 11.5 (since each condition can fail in at most one case). $\square$

We now construct suitable R -compliant representations by making Lemma 11.1 explicit in certain instances.

Lemma 11.8. *Every odd integer $m \geq 1458091$ admits an R -compliant representation of quality at least $\frac{239}{7}$.*

Proof. Note first that 3 admits the R -compliant representation $z^2 - z + 1$ of quality at least $\frac{6}{7}$. Meanwhile, by Lemma 11.1(c), every positive odd integer $m \geq 486031$ admits a compliant representation $Q(z)$ of quality at least $\frac{296}{7}$. For such m and Q , $(z^2 - z + 1)Q(z)$ is an R -compliant representation of $3m$ of quality at least $\frac{6}{7} \cdot \frac{296}{7} > \frac{253}{7}$, and so $(z^2 - z + 1)Q(z) \pm 2$ is an R -compliant representation of $3m \pm 2$ of quality at least $\frac{253}{7} - 2 = \frac{239}{7}$. We thus deduce the claim for all $m \geq 3 \cdot 486031 - 2 = 1458091$. $\square$

To close the gap left by Lemma 11.8, we make some explicit computations of compliant representations.

Lemma 11.9. *Every odd positive integer $m \notin \{1, 5, 13, 19\}$ admits an R -compliant representation.*

Proof. We first prove the claim for $m \geq 9375$. By Lemma 10.2 and Lemma 10.3, every odd integer $m \geq 3123$ admits a compliant representation $Q(z)$ of quality at least $\frac{33}{7}$. For such m and Q , $(z^2 - z + 1)Q(z)$ is an R -compliant representation of $3m$ of quality at least $\frac{6 \cdot 33}{49} > 4$. Consequently, $3m \pm 2$ admits the R -compliant representations $(z^2 - z + 1)Q(z) \pm 2$.

To close the range, we adapt the proof of Lemma 10.2 as follows. We first run an exhaust over monic polynomials Q of degree at most 8 with all coefficients in $\{-3, \dots, 3\}$ and $m = Q(0)$ odd, checking whether Q is an R -compliant representation of m . We then combine with the result of the computation proving Lemma 10.2, then look for additional R -compliant representations for $m \leq 101000$ using the following logic: if Q_1 is a compliant representation of an odd integer m_1 of quality q_1 , Q_2 is an R -compliant representation of an odd integer m_2 of quality q_2 , and $c \equiv 0 \pmod{2}$ is an integer with $q_1 q_2 > |c|$, then $R(z) = Q_1(z)Q_2(z) + c$ is an R -compliant representation of $m_1 m_2 + c$ of quality at least $q_1 q_2 - |c|$. This in particular yields R -compliant representations of all odd m with $1 < m \leq 9375$ and $m \notin \{5, 13, 19\}$. $\square$

We then extend Lemma 11.8 as follows.

Lemma 11.10. *For m odd with $70054 \leq m \leq 1458090$, m admits an R -compliant representation of quality at least $\frac{239}{7}$.*

Proof. For $350000 \leq m \leq 1458090$, we write $m = 15m_0 + c$ with m_0 odd and $|c| \leq 14$. We then consult the computation made in Lemma 11.9 to obtain an R -compliant representation $Q(z)$ of m_0 , then verify that in each case $\text{qual}((z^4 - 1)Q(z) + c) \geq \frac{239}{7}$.

For $101000 \leq m \leq 350000$, we write $m = 3m_0 + c$ with m_0 odd and $|c| \leq 2$. We then consult the computation made in Lemma 10.2 to obtain a compliant representation $Q(z)$ of m_0 , then verify that in each case $\text{qual}((z^2 - z + 1)Q(z) + c) \geq \frac{239}{7}$.

For $70054 \leq m \leq 101000$, we consult the computation made in Lemma 11.9 to obtain an R -compliant representation $Q(z)$ of m_0 , then verify that in each case $\text{qual}(Q(z)) \geq \frac{239}{7}$. $\square$

Lemma 11.11. *For m odd (but not necessarily prime) with $m \leq 70054$ and*

$$m \notin \{3, 5, 11, 13, 15, 19, 25, 27, 35, 57, 81, 87, 93, 95, 485\},$$

m admits an R -compliant representation to which the criterion of Lemma 11.3 applies.

Proof. We look up the R -compliant representation $Q(z)$ of m found in Lemma 11.9 and check whether it has quality at least $\frac{239}{7}$, in which case Lemma 11.6 again applies. Otherwise, we check directly whether $Q(z)$ satisfies the hypothesis of Lemma 11.3; when this fails, we try again using $Q(z) + 2i(z - 2)$ for $i \in \{\pm 1, \pm z, \pm z^2\}$ (in each case first checking whether or not this is an R -compliant representation). This covers all asserted cases. $\square$

Theorem 11.12. *Conjecture 1.2 holds when m is an odd prime and $m \notin \{3, 5, 11, 13, 19\}$.*

Proof. It suffices to show that for each such m , there is an R -compliant representation to which Lemma 11.3 applies. For $m \geq 1458090$, this follows from Lemma 11.6 and Lemma 11.8. For $70054 \leq m \leq 1458090$, this follows from Lemma 11.6 and Lemma 11.10. For $m \leq 70054$, this follows from Lemma 11.11. $\square$

12 Odd prime power orders: large cases

We next adapt the proof of Theorem 11.12 to handle the case where m is a higher power of an odd prime p , by incorporating the analysis of Newton polygons from the proof of Theorem 9.3. The relevant analogue of Lemma 12.1 is the following.

Lemma 12.1. *Let $Q(-z)$ be an R -compliant representation of an odd positive integer m of degree d to which the criterion of Lemma 12.1 applies, and for which $Q'(-2)$ is coprime to m . If m is a power of a prime p , then Conjecture 1.2 holds for m .*

Proof. By (4.10), the condition that $Q'(-2)$ is coprime to p ensures that for $n \geq d + 2$, the linear coefficient of P_n is coprime to p , and so the p -adic Newton polygon of $P_n(x)$ has a single nonzero slope. As in the proof of Theorem 9.3, this ensures that the only way for $P_n(x)$ to factor nontrivially is for it to have an irreducible factor with constant coefficient ± 1 ; we may thus continue as in the proof of Lemma 11.3 to conclude. $\square$

For p large enough, we obtain a direct analogue of Lemma 11.6.

Lemma 12.2. *Let m be a power of a prime $p > 7$. Suppose that m admits an R -compliant representation $Q(z)$ of quality at least $\frac{239}{7}$. Then Conjecture 1.2 holds for m .*

Proof. With notation as in the proof of Lemma 11.6, the nonvanishing of $Q'(2) \pmod{p}$ may be added as a tenth condition which fails for at most one of the 11 polynomials in the set (11.7); we thus obtain at least one polynomial satisfying the criterion of Lemma 12.1. $\square$

Theorem 12.3. *Conjecture 1.2 holds when m is a higher power of a prime $p > 7$.*

Proof. Combining Lemma 12.2, Lemma 11.8, and Lemma 11.10 proves the claim whenever $m \geq 70054$. For $m \leq 70054$, we repeat the computation of Lemma 11.11, adding the condition that when m is a power of a prime $p > 7$, the criterion of Lemma 12.1 holds. This resolves all remaining cases. $\square$

For $p \leq 7$, we need to modify the method of Lemma 12.2 slightly.

Lemma 12.4. *Let m be a power of $p \in \{5, 7\}$ (resp. of $p = 3$). Suppose that m admits an R -compliant representation $Q(z)$ of quality at least 41 (resp. $\frac{335}{7}$). Then Conjecture 1.2 holds for m .*

Proof. The proof of Lemma 12.2 applies if we replace the range $-5, \dots, 5$ with $-6, \dots, 6$ (resp. $-7, \dots, 7$) in (11.7): we then have a set of 13 (resp. 15) polynomials, of which at most 9 are excluded by Remark 11.5, and the remaining candidates are too numerous to fit into a single residue class modulo p . $\square$

Theorem 12.5. *Conjecture 1.2 holds when m is a power of a prime $p \in \{3, 5, 7\}$ with $m > 100$.*

Proof. By Lemma 11.1, any odd $m \geq 7290451$ has a compliant representation of quality at least $\frac{790}{7}$; as in Lemma 11.8, this ensures that $3m$ and $3m \pm 2$ have compliant representations of quality at least $\frac{663}{7}$. By Lemma 12.4, this covers all cases where $m = 3^e$ with $e \geq 15$, $m = 5^e$ with $e \geq 10$, and $m = 7^e$ with $e \geq 9$.

For $p = 7$ and $m = p^e$ with $3 \leq e \leq 8$, $p = 5$ and $m = p^e$ with $5 \leq e \leq 9$, or $p = 3$ and $m = p^e$ with $6 \leq e \leq 14$, we exhibit an R -compliant representation $Q(z)$ of m such that $Q(z) \pm 2(z - 2)$ satisfies the criterion of Lemma 12.1; more precisely, $Q(z)$ is a product of an R -compliant representation of some power of p with a power of a compliant representation of p . For $m = 3^5$, we make a similar construction using $Q(z) + 2z(z - 2)$. This accounts for all claimed cases. $\square$

13 Remarks on odd composite orders

We do not presently have a way to resolve Conjecture 1.2 for any single odd m which is not a prime or a higher prime power. Here is our best partial result.

Theorem 13.1. *Let m be an odd positive integer which is not a power of a prime. Then there exists a sequence $\{P_n(x)\}$ of polynomials satisfying (3.1) such that for $n \gg 0$, $|P_n(0)| = m$ and $P_n(x)$ has no irreducible factor $S(x)$ with $S(0) = \pm 1$.*

Proof. From the proof of Theorem 11.12, every odd integer $m \geq 70054$ admits an R -compliant representation to which Lemma 11.3 applies. Combining this with Lemma 11.11, we deduce the claim in all cases except

$$m \in \{15, 35, 57, 87, 93, 95, 485\}.$$

In these cases, we exhibit an explicit pair $P_0(x), P_1(x)$ which satisfy the hypotheses of Theorem 6.2 (see Table 4). In all cases, the mod-2 reductions of the resulting polynomials $P_n(x)$ are of the shape to which either Lemma 8.4 or Lemma 8.5 applies; using Lemma 3.11(a), we deduce that an irreducible factor $S(x)$ with $S(0) = \pm 1$ would have to satisfy $k \leq 30$. We may then rule this out by testing that P_n is irreducible for $n = 0, \dots, 29$. $\square$

Unfortunately, when m is not a power of a prime, we have no strategy in mind to rule out irreducible factors $S(x)$ for which $|S(0)|$ is a proper divisor of m greater than 1. Lemma 3.10 implies that any such S can occur for at most one n , but there are infinitely many S that need to be excluded.

In [3], it was established that any sequence of polynomials $P_n(x)$ arising from a compliant representation of an odd positive integer includes infinitely many distinct irreducible factors; this was done by considering the 2-adic Newton polygons of $P_n(x+1)$ rather than $P_n(x)$, and showing that in infinitely many cases one obtains a segment whose complement is of bounded multiplicity. However, due to the nature of the recurrence (3.1), such a construction can only work for an exponentially thin sequence of degrees.

This suggests dropping the constraint that the polynomials occur in a single recurrent sequence. Some experiments suggest that one can quite often find monic integer polynomials $P(x)$ with all roots in $[a, b]$ such that $|P(0)| = m$, $|P(1)| = 2$, and $P(x+1) \equiv x^{\deg(P)} \pmod{2}$; when this occurs, we can deduce that $P(x+1)$ is irreducible over $\mathbb{Q}_2$, as then is P . (The congruence condition is equivalent to the condition that the corresponding abelian variety has 2-rank 0.) However, we were unable to make this systematic; for $m = 3$, such polynomials P exist with $\deg(P) = 1, \dots, 8$ but not with $\deg(P) = 9$. It might be feasible to construct polynomials satisfying a slightly weaker congruence condition that still ensures that P has a 2-adic irreducible factor with bounded codegree, but we must be careful as we do not have Lemma 3.10 in this context.

An alternate approach would be to ensure that $|P(-1)|$ is prime, as a factor S of P cannot satisfy $|S(-1)| = 1$ unless S is constant. It is not yet clear whether there exist enough polynomials with fixed constant term and all roots in $[a, b]$ to make this feasible. See [4] for some first steps towards analyzing the count of such polynomials.

m	$P_0(x)$
15	$x^2 - 7x + 9$
35	$x^3 - 10x^2 + 29x - 21$
57	$x^3 - 11x^2 + 38x - 41$
87	$x^4 - 13x^3 + 59x^2 - 108x + 63$
93	$x^4 - 14x^3 + 68x^2 - 133x + 89$
95	$x^4 - 13x^3 + 60x^2 - 116x + 79$
485	$x^5 - 18x^4 + 124x^3 - 405x^2 + 618x - 343$

m	$P_1(x)$
15	$x^3 - 9x^2 + 22x - 15$
35	$x^4 - 12x^3 + 48x^2 - 73x + 35$
57	$x^4 - 13x^3 + 58x^2 - 102x + 57$
87	$x^5 - 15x^4 + 83x^3 - 207x^2 + 226x - 87$
93	$x^5 - 16x^4 + 94x^3 - 246x^2 + 273x - 93$
95	$x^5 - 15x^4 + 84x^3 - 216x^2 + 248x - 95$
485	$x^6 - 20x^5 + 158x^4 - 624x^3 + 1281x^2 - 1278x + 485$

m	$P_n(x) \pmod{2}$
15	$x^{n+2} + x^{n+1} + 1$
35	$x^{n+3} + x + 1$
57	$x^{n+3} + x^{n+2} + 1$
87	$x^{n+4} + x^2 + x + 1$
93	$x^{n+4} + x + 1$
95	$x^{n+4} + x^{n+3} + 1$
485	$x^{n+5} + x^2 + 1$

Table 4: Polynomials used in the proof of Theorem 13.1.

A Sequences of polynomials with roots in an interval

The following appendix is meant to be readable independently of the rest of the paper; it is devoted to establishing a variant of [11, Theorem 1]. That theorem gives a condition for showing that certain second-order recurrent sequences of univariate polynomials consist entirely of polynomials with all real roots (e.g., sequences of orthogonal polynomials); our variant does the same for polynomials with all roots in a fixed interval. We demonstrate this with a few examples from OEIS [9].

Let $f(x)$ and $g(x)$ be real polynomials whose roots are all real; label these roots respectively as $\alpha_1 \leq \dots \leq \alpha_n$ and $\beta_1 \leq \dots \leq \beta_m$. We say that g *interlaces* f if $m = n - 1$ and

$$\alpha_1 \leq \beta_1 \leq \alpha_2 \leq \dots \leq \alpha_{n-1} \leq \beta_{n-1} \leq \alpha_n \quad (\text{A.1})$$

(interpreting the condition as being vacuously true when $n = 1$). We say that g *left alternates* f if $m = n$ and

$$\beta_1 \leq \alpha_1 \leq \beta_2 \leq \dots \leq \beta_n \leq \alpha_n. \quad (\text{A.2})$$

Theorem A.3. Choose real numbers A, B, C, D with $A \geq 0$ and real numbers $y \leq z$ with

$$Cy + D, Cz + D \leq 0, \quad (Ay + B)^2 + 4(Cy + D), (Az + B)^2 + 4(Cz + D) \geq 0;$$

then set

$$\alpha := \frac{Ay + B - \sqrt{(Ay + B)^2 + 4(Cy + D)}}{2}, \quad \beta := \frac{Az + B + \sqrt{(Az + B)^2 + 4(Cz + D)}}{2}.$$

Let f, g be real polynomials satisfying the following conditions.

- (i) The polynomials f and g have positive leading coefficients.
- (ii) The roots of f and g are all real and contained in $[y, z]$.
- (iii) The polynomial g interlaces f or left alternates f .
- (iv) We have

$$\liminf_{x \rightarrow y^+} \frac{f(x)}{g(x)} \leq \alpha, \quad \limsup_{x \rightarrow z^-} \frac{f(x)}{g(x)} \geq \beta.$$

Then the polynomial

$$h(x) := (Ax + B)f(x) + (Cx + D)g(x)$$

has positive leading coefficient; the roots of h are all real and contained in $[y, z]$; f interlaces h ; and

$$\liminf_{x \rightarrow y^+} \frac{h(x)}{f(x)} \leq \alpha, \quad \liminf_{x \rightarrow z^-} \frac{h(x)}{f(x)} \geq \beta.$$

Proof. Since removing a common monic factor from f and g affects neither the hypotheses nor the conclusion, we may assume without loss of generality that f and g have no common roots; this implies in particular that f has no repeated roots. We may also assume that C and D are not both zero, as otherwise $h(x) = (Ax + B)f(x)$ has the roots of f plus the root y .

By writing

$$\frac{h(x)}{f(x)} = Ax + B + (Cx + D) \frac{g(x)}{f(x)}, \quad (\text{A.4})$$

we see that

$$\begin{aligned} \frac{h(y)}{f(y)} &= Ay + b + (Cy + D) \frac{g(y)}{f(y)} \leq Ay + B + \frac{Cy + D}{\alpha} = \alpha \leq 0 \\ \frac{h(z)}{f(z)} &= Az + b + (Cz + D) \frac{g(z)}{f(z)} \geq Az + B + \frac{Cz + D}{\beta} = \beta \geq 0. \end{aligned}$$

Let c_f and c_g be the leading coefficients of f and g , respectively. Fix $i \in \{1, \dots, n\}$. If g interlaces f , then with notation as in (A.1),

$$\frac{h(x)}{f(x)} = Ax + B + \frac{Cx + D}{x - \alpha_i} \frac{c_f}{c_g} \prod_{j=1}^{i-1} \frac{\beta_j - x}{\alpha_i - x} \prod_{j=i}^{n-1} \frac{x - \beta_j}{x - \alpha_{i+1}}; \quad (\text{A.5})$$

if g left alternates f , then with notation as in (A.2),

$$\frac{h(x)}{f(x)} = Ax + B + \frac{Cx + D}{x - \alpha_i} (x - \beta_i) \frac{c_f}{c_g} \prod_{j=1}^{i-1} \frac{\beta_j - x}{\alpha_i - x} \prod_{j=i}^{n-1} \frac{x - \beta_{j+1}}{x - \alpha_{i+1}}. \quad (\text{A.6})$$

In both cases, the quantity $\frac{Cx+D}{x-\alpha_i}$ is multiplied by an expression in which every factor evaluates to a positive quantity at $x = \alpha_i$. Since $Cx + D < 0$ for $y < x < z$, we conclude that on each of the intervals

$$[y, \alpha_1), (\alpha_1, \alpha_2), \dots, (\alpha_{n-1}, \alpha_n), (\alpha_n, z], \quad (\text{A.7})$$

the function $\frac{h(x)}{f(x)}$ is continuous, has a negative limit at the left endpoint (or zero if the endpoint y is included), and has a positive limit at the right endpoint (or zero if the endpoint z is included). Using the intermediate value theorem and the fact that $\deg(h) \leq n + 1$, we deduce all of the desired properties of h . $\square$

We recover [11, Theorem 1] as follows.

Corollary A.8 (Wang–Yeh). *Choose real numbers A, B, C, D with $AD \leq BC$. Let f, g be real polynomials satisfying the following conditions.*

- (i) *The polynomials f and g have positive leading coefficients.*
- (ii) *The roots of f and g are all real.*
- (iii) *The polynomial g interlaces f or left alternates f .*

Then the roots of the polynomial

$$h(x) := (Ax + B)f(x) + (Cx + D)g(x)$$

are all real; moreover, if g interlaces f , then f interlaces h .

Proof. We may again assume that f and g have no common root (and so f has no repeated roots); by taking limits, we may further reduce to the case where $AD \neq 0$. We may also assume without loss of generality that $A > 0$.

We first treat the case where g interlaces f and $C = 0$; in this case $D < 0$. We may then apply Theorem A.3 with y arbitrarily small and z arbitrarily large to deduce the claim.

We next treat the case where g interlaces f and C is arbitrary. Set

$$\tilde{f}(x) = f(x) + \frac{C}{A}g(x), \quad \tilde{g}(x) = g(x);$$

then $\tilde{g}$ interlaces $\tilde{f}$ and

$$h(x) = (Ax + B)\tilde{f}(x) - \frac{BC - AD}{A}\tilde{g}(x),$$

so we may apply the previous case to conclude.

We finally treat the case where g left alternates f (by a reduction from the proof of [11, Theorem 1]). Set notation as in (A.2) and set

$$\tilde{f}(x) = g(x + \alpha_1), \quad \tilde{g}(x) = \tilde{f}(x + \alpha_1)/x, \quad \tilde{h}(x) = h(x + \alpha_1);$$

then $\tilde{g}$ interlaces $\tilde{f}$ and

$$\tilde{h}^* = (Cx + (C\alpha_1 + D))\tilde{f}(x) + (Ax + (A\alpha_1 + B))x\tilde{g}(x).$$

Let $\tilde{f}^*, \tilde{g}^*, \tilde{h}^*$ be the reversed polynomials of $\tilde{f}, \tilde{g}, \tilde{h}$; then $\tilde{g}^*$ again interlaces $\tilde{f}^*$ and

$$\tilde{h}^*(x) = ((C\alpha_1 + D)x + C)\tilde{f}^*(x) + ((A\alpha_1 + B)x + A)\tilde{g}^*(x).$$

By the previously treated case, the roots of $\tilde{h}^*$ are real and $\tilde{f}^*$ interlaces $\tilde{h}^*$; hence the roots of $\tilde{h}$ are real and $\tilde{f}$ interlaces $\tilde{h}$, from which we deduce the desired result. $\square$

One can also derive a similar result for polynomials with roots in a fixed one-sided interval. To simplify the statement, we restrict to the interlacing case; in the left alternating case, we would need two separate statements depending on whether the one-sided interval is bounded on the left or the right.

Corollary A.9. Choose real numbers A, B, C, D with $A \geq 0$, $C \leq 0$, and a real number y with

$$Cy + D \leq 0, \quad (Ay + B)^2 + 4(Cy + D) \geq 0;$$

then set

$$\alpha := \frac{Ay + B - \sqrt{(Ay + B)^2 + 4(Cy + D)}}{2}.$$

Let f, g be real polynomials satisfying the following conditions.

- (i) The polynomials f and g have positive leading coefficients.
- (ii) The roots of f and g are all real and contained in $[y, \infty)$.
- (iii) The polynomial g interlaces f .
- (iv) We have

$$\liminf_{x \rightarrow y^+} \frac{f(x)}{g(x)} \leq \alpha.$$

Then the polynomial

$$h(x) := (Ax + B)f(x) + (Cx + D)g(x)$$

has positive leading coefficient; the roots of h are all real and contained in $[y, \infty)$; f interlaces h ; and

$$\liminf_{x \rightarrow y^+} \frac{h(x)}{f(x)} \leq \alpha.$$

Proof. Since $Cz + D \rightarrow -\infty$ and $(Az + B)^2 + 4(Cz + D) \rightarrow +\infty$ as $z \rightarrow +\infty$, we may apply Theorem A.3 with z arbitrarily large to deduce the claim. $\square$

We apply these results to show that various sequences in OEIS correspond (up to signs and leading terms) to coefficients of sequences of polynomials $P_n(x)$ with interlaced roots and satisfying recurrence relations of the form

$$P_n(x) = (Ax + B)P_{n-1}(x) + (Cx + D)P_{n-2}(x)$$

for some real numbers A, B, C, D .

We first take $A = 1, B = 0, C = 0, D = -1$; in this case we obtain some sequences of orthogonal polynomials. For $|c| \leq 2$ we may apply Theorem A.3 with

$$y = -2, z = 2, \alpha = -1, \beta = 1 :$$

the case $c = 0$ (Chebyshev polynomials) corresponds to OEIS A053119 (see also A049310, AA104562); the case $c = 1$ corresponds to OEIS A108299; the case $c = 2$ corresponds to OEIS A374439. In passing, we note that for $c > 2$ we must instead take

$$y = -c - c^{-1}, z = 2, \alpha = -c^{-1}, \beta = 2,$$

and the resulting conclusion does not fully explain the resulting behavior: empirically it appears that $P_n(x)$ has one root very close to y and the others again in $[-2, 2]$.

We next take $A = 1, B = -1, C = -1, D = 0$ (as in (3.1) in the main text). In this case we obtain some sequences of *Laurent biorthogonal polynomials*. We apply Theorem A.3 with $y = 3 - 2\sqrt{2}, z = 3 + 2\sqrt{2}, \alpha = 1 - \sqrt{2}, \beta = 1 + 2\sqrt{2}$:

- the case $P_0(x) = 1, P_1(x) = x - 1$ corresponds to OEIS A008288;
- the case $P_0(x) = 1, P_1(x) = x - 2$ (used in Theorem 7.1 in the main text) corresponds to OEIS A035607;

- the case $P_0(x) = 1, P_1(x) = x - 3$ (used in Theorem 8.2 in the main text) corresponds to OEIS A102662;
- the case $P_0(x) = 2, P_1(x) = x - 1$ (called $f_n(x)$ in the main text) corresponds to OEIS A102413;
- the case $P_0(x) = x - 1, P_1(x) = x^2 - 2x + 1$ corresponds to OEIS A128966.

We next take $A = 1, D = 0$ but allow $B, C \geq 0$. For $P_0(x) = 1, P_1(x) = x + 1$, the coefficients of the resulting sequence form a *Delannoy-like triangle* in the terminology of [8]. As such, [8, Theorem 3] includes the assertion that $P_n(x)$ has all real roots, and the proof (using [6, Theorem 2.1]) even shows that any two consecutive polynomials in the sequence are interlaced. To locate the roots in an interval, it suffices to find y, z such that $(y + B)^2 + 4C, (z + B)^2 + 4C \geq 0$ and the resulting values

$$\alpha := \frac{y + B - \sqrt{(y + B)^2 + 4C}}{2}, \quad \beta := \frac{z + B + \sqrt{(z + B)^2 + 4C}}{2}$$

satisfy

$$y + 1 \leq \alpha, \quad z + 1 \geq \beta.$$

When $B \leq 2 + \frac{1}{B+C}$ (i.e., $B < 2$ and $C \geq \frac{1}{2-B} - B$), we may take

$$y = -B - 2C - 2\sqrt{C(B+C)}, \quad z = -B - 2C + 2\sqrt{C(B+C)}.$$

Otherwise, we must have $B + C > 1$ (otherwise $B \geq 3$ and hence $C \leq -2$), and we instead take

$$y = -B - 2C - 2\sqrt{C(B+C)}, \quad z = \frac{B + C - 1}{B - 1}.$$

We conclude by noting that [6, Theorem 2.1] gives an extension of [11, Theorem 1.1] which replaces the linear polynomials $Ax + B, Cx + D$ in the recurrence relation with more general polynomials (and as noted above includes the conclusion about interlacing). It would be of some interest to give (or perhaps identify in existing literature!) a variant of this result concerning polynomials with roots in a real interval; in fact it would suffice to treat the case of polynomials with nonnegative real roots.

References

- [1] Raymond van Bommel, Edgar Costa, Wanlin Li, Bjorn Poonen, and Alexander Smith. Abelian varieties of prescribed order over finite fields. *Mathematische Annalen*, 392:1167–1202, 2025. DOI: 10.1007/s00208-024-03084-4.
- [2] Toreen D’Nelly-Warady and Kiran S. Kedlaya. Geometric decomposition of abelian varieties of order 1. In *Research Directions in Number Theory*, volume 33 of *Association for Women in Mathematics Series*, pages 253–270. Springer, 2024. DOI: 10.1007/978-3-031-51677-1_8.

- [3] Kiran S. Kedlaya. Abelian varieties over $\mathbb{F}_2$ of prescribed order. In *Proceedings of the GTA 2021 Conference*, special volume of *Publications mathématiques de Besançon*, pages 43–58, 2024. doi: 10.5802/pmb.55.
- [4] Kiran S. Kedlaya. Distribution of Frobenius polynomials of abelian varieties of extremely small order. Preprint, 2025. <https://kskedlaya.org/papers/fixed-order-dist.pdf>.
- [5] Kiran S. Kedlaya, Alexander Kolpakov, Bjorn Poonen, and Michael Rubinstein. Space vectors forming rational angles. Preprint, 2020. doi: 10.48550/arXiv.2011.14232.
- [6] Lily L. Liu and Yi Wang. A unified approach to polynomial sequences with only real zeros. *Advances in Applied Mathematics*, 38(4):542–560, 2007. doi: 10.1016/j.aam.2006.02.003.
- [7] Manohar L. Madan and Sat Pal. Abelian varieties and a conjecture of R.M. Robinson. *Journal für die reine und angewandte Mathematik*, 291:78–91, 1977. doi: 10.1515/crll.1977.291.78.
- [8] Lili Mu and Sai-nan Zheng. On the total positivity of Delannoy-like triangles. *Journal of Integer Sequences*, 20:17.1.6, 2017.
- [9] OEIS Foundation. *The On-Line Encyclopedia of Integer Sequences*. <https://oeis.org/>.
- [10] Raphael M. Robinson. Conjugate algebraic units in a special interval. *Mathematische Zeitschrift*, 154:31–40, 1977. doi: 10.1007/BF01215110.
- [11] Yi Wang and Yeong-Nan Yeh. Polynomials with real zeros and Pólya frequency sequences. *Journal of Combinatorial Theory, Series A*, 109(1):63–74, 2005. doi: 10.1016/j.jcta.2004.07.008.