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

Kiran S. Kedlaya

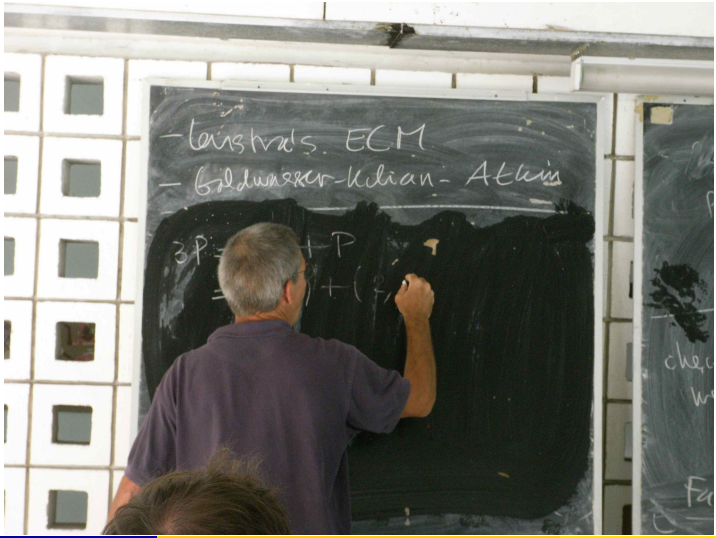
Department of Mathematics, University of California San Diego
kedlaya@ucsd.edu
These slides can be downloaded from https://kskedlaya.org/slides/.

René 25: Celebrating the research interests of René Schoof
Université de la Polynesie Française / Fare haʻapiʻiraʻa tuatoru nō Pōrinetia farāni
Punaʻauia, Tahiti, French Polynesia
August 22, 2025

Supported by NSF (grant DMS-2401536) and UC San Diego (Warschawski Professorship).

I acknowledge that my workplace occupies unceded ancestral land of the Kumeyaay Nation.

Bellairs, Barbados, 2008



Tetiaroa, earlier this week

Contents

The Weil bound

Throughout, let A be an abelian variety over a finite field $\mathbb{F}_q$. For $g := \dim(A)$, the Frobenius characteristic polynomial is a **Weil polynomial**, i.e., has the form

$$P_A(T) = (T - \alpha_1)(T - \overline{\alpha}_1) \cdots (T - \alpha_g)(T - \overline{\alpha}_g) \in \mathbb{Z}[T]$$

where $\alpha_1, \ldots, \alpha_g \in \mathbb{C}$ lie on the circle $|T| = q^{1/2}$ (Weil, 1940s).

We also have

$$\#A(\mathbb{F}_q) = P_A(1) = \prod_{i=1}^{g} (\alpha_i - 1)(\overline{\alpha}_i - 1).$$

Using the triangle inequality on each factor in the product, we get the Weil lower bound

$$\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}.$$

For fixed $q \geq 5$, this implies that $\#A(\mathbb{F}_q)$ grows exponentially with g.

The Weil bound

Throughout, let A be an abelian variety over a finite field $\mathbb{F}_q$. For $g := \dim(A)$, the Frobenius characteristic polynomial is a **Weil polynomial**, i.e., has the form

$$P_A(T) = (T - \alpha_1)(T - \overline{\alpha}_1) \cdots (T - \alpha_g)(T - \overline{\alpha}_g) \in \mathbb{Z}[T]$$

where $\alpha_1, \ldots, \alpha_g \in \mathbb{C}$ lie on the circle $|T| = q^{1/2}$ (Weil, 1940s).

We also have

$$\#A(\mathbb{F}_q) = P_A(1) = \prod_{i=1}^{g} (\alpha_i - 1)(\overline{\alpha}_i - 1).$$

Using the triangle inequality on each factor in the product, we get the Weil lower bound

$$\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}.$$

For fixed $q \geq 5$, this implies that $\#A(\mathbb{F}_q)$ grows exponentially with g.

The Weil bound

Throughout, let A be an abelian variety over a finite field $\mathbb{F}_q$. For $g := \dim(A)$, the Frobenius characteristic polynomial is a **Weil polynomial**, i.e., has the form

$$P_A(T) = (T - \alpha_1)(T - \overline{\alpha}_1) \cdots (T - \alpha_g)(T - \overline{\alpha}_g) \in \mathbb{Z}[T]$$

where $\alpha_1, \ldots, \alpha_g \in \mathbb{C}$ lie on the circle $|T| = q^{1/2}$ (Weil, 1940s).

We also have

$$\#A(\mathbb{F}_q) = P_A(1) = \prod_{i=1}^{g} (\alpha_i - 1)(\overline{\alpha}_i - 1).$$

Using the triangle inequality on each factor in the product, we get the Weil lower bound

$$\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}.$$

For fixed $q \geq 5$, this implies that $\#A(\mathbb{F}_q)$ grows exponentially with g.

The situation for small q

For $q \leq 4$, there is no such lower bound because there exists an elliptic curve E with $\#E(\mathbb{F}_q) = 1$. For any g, $A := E^g$ satisfies $\#A(\mathbb{F}_q) = 1$.

For $q = 3, 4$, we still get an exponential lower bound for **simple** A (Aubry–Haloui–Lachaud, 2013; Kadets, 2021; van Bommel–Costa–Li–Poonen–Smith, 2025).

For $q = 2$, there are **infinitely many** simple A of order 1 (Madan–Pal, 1975). In fact:

Theorem (K., 2021, 2025; the ostensible subject of this talk)

For any positive integer m, there exist infinitely many simple abelian varieties A over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = m$. When m is even or a power of an odd prime, these exist in **every** *sufficiently large dimension.*

The first assertion was (supposed to have been) presented at GTA (Tahiti, 2021). However, the delay to this occasion is perhaps fitting...

The situation for small q

For $q \leq 4$, there is no such lower bound because there exists an elliptic curve E with $\#E(\mathbb{F}_q) = 1$. For any g, $A := E^g$ satisfies $\#A(\mathbb{F}_q) = 1$.

For $q = 3, 4$, we still get an exponential lower bound for **simple** A (Aubry–Haloui–Lachaud, 2013; Kadets, 2021; van Bommel–Costa–Li–Poonen–Smith, 2025).

For $q = 2$, there are **infinitely many** simple A of order 1 (Madan–Pal, 1975). In fact:

Theorem (K., 2021, 2025; the ostensible subject of this talk)

For any positive integer m, there exist infinitely many simple abelian varieties A over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = m$. When m is even or a power of an odd prime, these exist in **every** *sufficiently large dimension.*

The first assertion was (supposed to have been) presented at GTA (Tahiti, 2021). However, the delay to this occasion is perhaps fitting...

The situation for small q

For $q \leq 4$, there is no such lower bound because there exists an elliptic curve E with $\#E(\mathbb{F}_q) = 1$. For any g, $A := E^g$ satisfies $\#A(\mathbb{F}_q) = 1$.

For $q = 3, 4$, we still get an exponential lower bound for **simple** A (Aubry–Haloui–Lachaud, 2013; Kadets, 2021; van Bommel–Costa–Li–Poonen–Smith, 2025).

For $q = 2$, there are **infinitely many** simple A of order 1 (Madan–Pal, 1975). In fact:

Theorem (K., 2021, 2025; the ostensible subject of this talk)

For any positive integer m, there exist infinitely many simple abelian varieties A over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = m$. When m is even or a power of an odd prime, these exist in **every** *sufficiently large dimension.*

The first assertion was (supposed to have been) presented at GTA (Tahiti, 2021). However, the delay to this occasion is perhaps fitting...

The situation for small q

For $q \leq 4$, there is no such lower bound because there exists an elliptic curve E with $\#E(\mathbb{F}_q) = 1$. For any g, $A := E^g$ satisfies $\#A(\mathbb{F}_q) = 1$.

For $q = 3, 4$, we still get an exponential lower bound for **simple** A (Aubry–Haloui–Lachaud, 2013; Kadets, 2021; van Bommel–Costa–Li–Poonen–Smith, 2025).

For $q = 2$, there are **infinitely many** simple A of order 1 (Madan–Pal, 1975). In fact:

Theorem (K., 2021, 2025; the ostensible subject of this talk)

For any positive integer m, there exist infinitely many simple abelian varieties A over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = m$. When m is even or a power of an odd prime, these exist in **every** *sufficiently large dimension.*

The first assertion was (supposed to have been) presented at GTA (Tahiti, 2021). However, the delay to this occasion is perhaps fitting...

Context: relative class number problems

Leitzel–Madan–Queen (1975) showed that there are **seven** isomorphism classes of function fields (of curves over arbitrary finite fields) of positive genus with class number 1...

... allegedly. However, while completing his PhD thesis under Schoof, Stirpe (2014) discovered an eighth! Then Mercuri–Stirpe (2015) and Shen–Shi (2015) showed independently that the new list is complete.

Using some knowledge about abelian varieties of order 1, one can also solve the **relative** class number one problem for function fields (K., 2022–2025). The point is that for $C' \to C$ a finite morphism of curves over $\mathbb{F}_q$, the Prym variety $A := A_{C' \to C}$ has the property that

$$\frac{h_{C'}}{h_C} = \#A(\mathbb{F}_q).$$

Warning: some complications arise from the fact that A need not be simple.

One can similarly give an effective upper bound for the relative class number m problem for any fixed m (Arango-Piñeros–Chara–Hamakiotes–K.–Rama, 2025; see my AGC^{2}T 2025 talk).

Context: relative class number problems

Leitzel–Madan–Queen (1975) showed that there are **seven** isomorphism classes of function fields (of curves over arbitrary finite fields) of positive genus with class number 1...

... allegedly. However, while completing his PhD thesis under Schoof, Stirpe (2014) discovered an eighth! Then Mercuri–Stirpe (2015) and Shen–Shi (2015) showed independently that the new list is complete.

Using some knowledge about abelian varieties of order 1, one can also solve the **relative** class number one problem for function fields (K., 2022–2025). The point is that for $C' \to C$ a finite morphism of curves over $\mathbb{F}_q$, the Prym variety $A := A_{C' \to C}$ has the property that

$$\frac{h_{C'}}{h_C} = \#A(\mathbb{F}_q).$$

Warning: some complications arise from the fact that A need not be simple.

One can similarly give an effective upper bound for the relative class number m problem for any fixed m (Arango-Piñeros–Chara–Hamakiotes–K.–Rama, 2025; see my AGC^{2}T 2025 talk).

Context: relative class number problems

Leitzel–Madan–Queen (1975) showed that there are **seven** isomorphism classes of function fields (of curves over arbitrary finite fields) of positive genus with class number 1...

... allegedly. However, while completing his PhD thesis under Schoof, Stirpe (2014) discovered an eighth! Then Mercuri–Stirpe (2015) and Shen–Shi (2015) showed independently that the new list is complete.

Using some knowledge about abelian varieties of order 1, one can also solve the **relative** class number one problem for function fields (K., 2022–2025). The point is that for $C' \to C$ a finite morphism of curves over $\mathbb{F}_q$, the Prym variety $A := A_{C' \to C}$ has the property that

$$\frac{h_{C'}}{h_C} = \#A(\mathbb{F}_q).$$

Warning: some complications arise from the fact that A need not be simple.

One can similarly give an effective upper bound for the relative class number m problem for any fixed m (Arango-Piñeros–Chara–Hamakiotes–K.–Rama, 2025; see my AGC^{2}T 2025 talk).

Context: relative class number problems

Leitzel–Madan–Queen (1975) showed that there are **seven** isomorphism classes of function fields (of curves over arbitrary finite fields) of positive genus with class number 1...

... allegedly. However, while completing his PhD thesis under Schoof, Stirpe (2014) discovered an eighth! Then Mercuri–Stirpe (2015) and Shen–Shi (2015) showed independently that the new list is complete.

Using some knowledge about abelian varieties of order 1, one can also solve the **relative** class number one problem for function fields (K., 2022–2025). The point is that for $C' \to C$ a finite morphism of curves over $\mathbb{F}_q$, the Prym variety $A := A_{C' \to C}$ has the property that

$$\frac{h_{C'}}{h_C} = \#A(\mathbb{F}_q).$$

Warning: some complications arise from the fact that A need not be simple.

One can similarly give an effective upper bound for the relative class number m problem for any fixed m (Arango-Piñeros–Chara–Hamakiotes–K.–Rama, 2025; see my AGC^{2}T 2025 talk).

Contents

Translation via Honda–Tate

Hereafter fix $q = 2$. By Honda–Tate,[1] every Weil polynomial over $\mathbb{F}_2$ is the Frobenius characteristic polynomial of some abelian variety (determined up to isogeny). Moreover, irreducible Weil polynomials correspond exactly to simple abelian varieties. We can thus forget about abelian varieties and rephrase:

Theorem (K, 2021, 2025; the more accurate subject of this talk)

For any positive integer m, there exist infinitely many irreducible Weil polynomials $P(T)$ over $\mathbb{F}_2$ with $P(1) = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large even degree.*

[1] This is not specific to $q = 2$: it holds as written for any prime q, and with a tweak for higher prime powers.

Translation via Honda–Tate

Hereafter fix $q = 2$. By Honda–Tate,[1] every Weil polynomial over $\mathbb{F}_2$ is the Frobenius characteristic polynomial of some abelian variety (determined up to isogeny). Moreover, irreducible Weil polynomials correspond exactly to simple abelian varieties. We can thus forget about abelian varieties and rephrase:

Theorem (K, 2021, 2025; the more accurate subject of this talk)

For any positive integer m, there exist infinitely many irreducible Weil polynomials $P(T)$ over $\mathbb{F}_2$ with $P(1) = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large even degree.*

[1] This is not specific to $q = 2$: it holds as written for any prime q, and with a tweak for higher prime powers.

Real Weil polynomials

Given a Weil polynomial $P(T)$ over $\mathbb{F}_2$, factored over $\mathbb{C}$ as

$$P(T) = (T - \alpha_1)(T - \overline{\alpha}_1) \cdots (T - \alpha_g)(T - \overline{\alpha}_g),$$

define $\beta_i := \alpha_i + \overline{\alpha}_i \in [-2\sqrt{2}, 2\sqrt{2}]$. Then the associated **real Weil polynomial**

$$Q(T) = (T - \beta_1) \cdots (T - \beta_g)$$

has integer coefficients and all complex roots in $[-2\sqrt{2}, 2\sqrt{2}]$, and can be used to recover P by writing $P(T) = T^g Q(T + 2T^{-1})$. Moreover, P is irreducible iff Q is.

By rewriting

$$(1 - \alpha_i)(1 - \overline{\alpha}_i) = 1 - \alpha_i - \overline{\alpha}_i + q = 3 - \beta_i,$$

we deduce that $P(1) = Q(3)$.

Real Weil polynomials

Given a Weil polynomial $P(T)$ over $\mathbb{F}_2$, factored over $\mathbb{C}$ as

$$P(T) = (T - \alpha_1)(T - \overline{\alpha}_1) \cdots (T - \alpha_g)(T - \overline{\alpha}_g),$$

define $\beta_i := \alpha_i + \overline{\alpha}_i \in [-2\sqrt{2}, 2\sqrt{2}]$. Then the associated **real Weil polynomial**

$$Q(T) = (T - \beta_1) \cdots (T - \beta_g)$$

has integer coefficients and all complex roots in $[-2\sqrt{2}, 2\sqrt{2}]$, and can be used to recover P by writing $P(T) = T^g Q(T + 2T^{-1})$. Moreover, P is irreducible iff Q is.

By rewriting

$$(1 - \alpha_i)(1 - \overline{\alpha}_i) = 1 - \alpha_i - \overline{\alpha}_i + q = 3 - \beta_i,$$

we deduce that $P(1) = Q(3)$.

A key shift

Let us instead consider $R(x) := (-1)^{\deg(Q)} Q(3-x)$. Then $R(x)$ is a monic (and irreducible if Q is) polynomial with integer coefficients having all complex roots in

$$[a, b] := [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$$

and we would like to ensure that $\#A(\mathbb{F}_2) = Q(3) = (-1)^{\deg(R)} R(0)$ takes a particular value.

Theorem (K, 2021, 2025; the most accurate subject of this talk)

For any positive integer m, there exist infinitely many monic irreducible polynomials $R(T)$ with integer coefficients with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and $|R(0)| = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large degree.*

A key shift

Let us instead consider $R(x) := (-1)^{\deg(Q)} Q(3-x)$. Then $R(x)$ is a monic (and irreducible if Q is) polynomial with integer coefficients having all complex roots in

$$[a, b] := [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$$

and we would like to ensure that $\#A(\mathbb{F}_2) = Q(3) = (-1)^{\deg(R)} R(0)$ takes a particular value.

Theorem (K, 2021, 2025; the most accurate subject of this talk)

For any positive integer m, there exist infinitely many monic irreducible polynomials $R(T)$ with integer coefficients with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and $|R(0)| = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large degree.*

The case of order 1

When $|R(0)| = 1$, Madan–Pal observed that for any root γ of $R(x)$, $\gamma + \gamma^{-1} - 4$ is an algebraic integer with all conjugates in $[-2, 2]$. By Kronecker, this must equal $\zeta + \zeta^{-1}$ for some root of unity ζ; running this backward, we generate infinitely many simple abelian varieties over $\mathbb{F}_2$ of order 1.

In the process, we also classify the real Weil polynomials of **all** such abelian varieties. In particular, with a handful of exceptions,[2] their degrees are the degrees of cyclotomic polynomials (i.e., the image of Euler ϕ); hence they do not occur in **every** sufficiently large degree.

When $|R(0)| = m > 1$, we cannot hope for a similar classification. However, the classification for $m = 1$ contains some structure that does persist for $m > 1$.

[2] These correspond to ζ of order 2, 7, 30.

The case of order 1

When $|R(0)| = 1$, Madan–Pal observed that for any root γ of $R(x)$, $\gamma + \gamma^{-1} - 4$ is an algebraic integer with all conjugates in $[-2, 2]$. By Kronecker, this must equal $\zeta + \zeta^{-1}$ for some root of unity ζ; running this backward, we generate infinitely many simple abelian varieties over $\mathbb{F}_2$ of order 1.

In the process, we also classify the real Weil polynomials of **all** such abelian varieties. In particular, with a handful of exceptions,[2] their degrees are the degrees of cyclotomic polynomials (i.e., the image of Euler ϕ); hence they do not occur in **every** sufficiently large degree.

When $|R(0)| = m > 1$, we cannot hope for a similar classification. However, the classification for $m = 1$ contains some structure that does persist for $m > 1$.

[2] These correspond to ζ of order 2, 7, 30.

The case of order 1

When $|R(0)| = 1$, Madan–Pal observed that for any root γ of $R(x)$, $\gamma + \gamma^{-1} - 4$ is an algebraic integer with all conjugates in $[-2, 2]$. By Kronecker, this must equal $\zeta + \zeta^{-1}$ for some root of unity ζ; running this backward, we generate infinitely many simple abelian varieties over $\mathbb{F}_2$ of order 1.

In the process, we also classify the real Weil polynomials of **all** such abelian varieties. In particular, with a handful of exceptions,[2] their degrees are the degrees of cyclotomic polynomials (i.e., the image of Euler ϕ); hence they do not occur in **every** sufficiently large degree.

When $|R(0)| = m > 1$, we cannot hope for a similar classification. However, the classification for $m = 1$ contains some structure that does persist for $m > 1$.

[2] These correspond to ζ of order 2, 7, 30.

The case of order 1

When $|R(0)| = 1$, Madan–Pal observed that for any root γ of $R(x)$, $\gamma + \gamma^{-1} - 4$ is an algebraic integer with all conjugates in $[-2, 2]$. By Kronecker, this must equal $\zeta + \zeta^{-1}$ for some root of unity ζ; running this backward, we generate infinitely many simple abelian varieties over $\mathbb{F}_2$ of order 1.

In the process, we also classify the real Weil polynomials of **all** such abelian varieties. In particular, with a handful of exceptions,[2] their degrees are the degrees of cyclotomic polynomials (i.e., the image of Euler ϕ); hence they do not occur in **every** sufficiently large degree.

When $|R(0)| = m > 1$, we cannot hope for a similar classification. However, the classification for $m = 1$ contains some structure that does persist for $m > 1$.

[2] These correspond to ζ of order 2, 7, 30.

Contents

A key recurrence relation

By a **good sequence**,[3] I will mean a sequence of monic integer polynomials $\{P_n(x)\}_{n=k}^{\infty}$ with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ satisfying the equation[4]

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

This implies $P_n(0) = -P_{n-1}(0)$; hence $|P_n(0)|$ is constant for $n > k$.

The key ingredient to prove the theorem is exhibiting some good sequences with $|P_n(0)| = m$. There then remains the subtlety of controlling irreducible factors.

For this, we exploit the 2-adic behavior of good sequences. For starters, every solution of the recurrence has mod-2 reduction of the form $A + Bx^n$ for some rational functions A, B. (In fact $x^k(x-1)A, x^k(x-1)B$ are polynomials for some k.)

[3] This terminology is not used in the papers.

[4] This looks like a recurrence for orthogonal polynomials, except that the coefficient of $P_{n-2}(x)$ is not 1 (so we cannot run the recurrence in reverse). Nonetheless this analogy may be helpful.

A key recurrence relation

By a **good sequence**,[3] I will mean a sequence of monic integer polynomials $\{P_n(x)\}_{n=k}^{\infty}$ with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ satisfying the equation[4]

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

This implies $P_n(0) = -P_{n-1}(0)$; hence $|P_n(0)|$ is constant for $n > k$.

The key ingredient to prove the theorem is exhibiting some good sequences with $|P_n(0)| = m$. There then remains the subtlety of controlling irreducible factors.

For this, we exploit the 2-adic behavior of good sequences. For starters, every solution of the recurrence has mod-2 reduction of the form $A + Bx^n$ for some rational functions A, B. (In fact $x^k(x-1)A, x^k(x-1)B$ are polynomials for some k.)

[3] This terminology is not used in the papers.

[4] This looks like a recurrence for orthogonal polynomials, except that the coefficient of $P_{n-2}(x)$ is not 1 (so we cannot run the recurrence in reverse). Nonetheless this analogy may be helpful.

A key recurrence relation

By a **good sequence**,[3] I will mean a sequence of monic integer polynomials $\{P_n(x)\}_{n=k}^{\infty}$ with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ satisfying the equation[4]

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

This implies $P_n(0) = -P_{n-1}(0)$; hence $|P_n(0)|$ is constant for $n > k$.

The key ingredient to prove the theorem is exhibiting some good sequences with $|P_n(0)| = m$. There then remains the subtlety of controlling irreducible factors.

For this, we exploit the 2-adic behavior of good sequences. For starters, every solution of the recurrence has mod-2 reduction of the form $A + Bx^n$ for some rational functions A, B. (In fact $x^k(x-1)A, x^k(x-1)B$ are polynomials for some k.)

[3] This terminology is not used in the papers.

[4] This looks like a recurrence for orthogonal polynomials, except that the coefficient of $P_{n-2}(x)$ is not 1 (so we cannot run the recurrence in reverse). Nonetheless this analogy may be helpful.

A key recurrence relation

By a **good sequence**,[3] I will mean a sequence of monic integer polynomials $\{P_n(x)\}_{n=k}^{\infty}$ with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ satisfying the equation[4]

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

This implies $P_n(0) = -P_{n-1}(0)$; hence $|P_n(0)|$ is constant for $n > k$.

The key ingredient to prove the theorem is exhibiting some good sequences with $|P_n(0)| = m$. There then remains the subtlety of controlling irreducible factors.

For this, we exploit the 2-adic behavior of good sequences. For starters, every solution of the recurrence has mod-2 reduction of the form $A + Bx^n$ for some rational functions A, B. (In fact $x^k(x-1)A, x^k(x-1)B$ are polynomials for some k.)

[3] This terminology is not used in the papers.

[4] This looks like a recurrence for orthogonal polynomials, except that the coefficient of $P_{n-2}(x)$ is not 1 (so we cannot run the recurrence in reverse). Nonetheless this analogy may be helpful.

Examples of good sequences

There is a good sequence $\{f_n\}$ starting with $f_0(x) = 2, f_1(x) = x - 1$. Then

$$f_2(x) = x^2 - 4x + 1, \quad f_3(x) = x^6 - 6x^2 + 6x - 1, \quad \ldots.$$

These behave like Chebyshev polynomials: the irreducible factors of the terms of the sequence correspond precisely to simple abelian varieties of order 1.

For $k \geq 0$, there is a sequence $\{g_{n,k}\}$ with

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

This is a good sequence with $g_{n,k}(0) = (-1)^n 2^k$.

Examples of good sequences

There is a good sequence $\{f_n\}$ starting with $f_0(x) = 2, f_1(x) = x - 1$. Then

$$f_2(x) = x^2 - 4x + 1, \quad f_3(x) = x^6 - 6x^2 + 6x - 1, \quad \ldots.$$

These behave like Chebyshev polynomials: the irreducible factors of the terms of the sequence correspond precisely to simple abelian varieties of order 1.

For $k \geq 0$, there is a sequence $\{g_{n,k}\}$ with

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

This is a good sequence with $g_{n,k}(0) = (-1)^n 2^k$.

Examples of good sequences

There is a good sequence $\{f_n\}$ starting with $f_0(x) = 2, f_1(x) = x - 1$. Then

$$f_2(x) = x^2 - 4x + 1, \quad f_3(x) = x^6 - 6x^2 + 6x - 1, \quad \ldots.$$

These behave like Chebyshev polynomials: the irreducible factors of the terms of the sequence correspond precisely to simple abelian varieties of order 1.

For $k \geq 0$, there is a sequence $\{g_{n,k}\}$ with

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

This is a good sequence with $g_{n,k}(0) = (-1)^n 2^k$.

A lemma on interlaced polynomials

Lemma

Let $P_0, P_1, \dots$ be real polynomials with $P_n(x) - (x-1)P_{n-1}(x) + xP_{n-2}(x) = 0$ and:

1. *P_1 is monic, P_0 has positive leading coefficient, and $\deg(P_1) = \deg(P_0) + 1$.*
2. *The roots of P_0 and P_1 are simple, contained in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$, and* **interlaced***: we can label the roots of P_1 as $\alpha_0, \dots, \alpha_d$ and the roots of P_0 as $\beta_1, \dots, \beta_d$ so that they alternate:*
$$\alpha_0 < \beta_1 < \alpha_1 < \cdots < \beta_d < \alpha_d.$$
3. *We have*
$$\frac{P_1(a)}{P_0(a)} \leq 1 - \sqrt{2}, \qquad \frac{P_1(b)}{P_0(b)} \geq 1 + \sqrt{2}.$$

Then for every $n \geq 0$, the roots of P_n and P_{n+1} are simple, contained in $[a, b]$, and interlaced.

A construction of sequences

Lemma (inspired by van Bommel–Costa–Poonen–Li–Smith)

Let $Q(z) := \sum_{i=0}^{k} a_i z^i$ be a monic real polynomial with all roots in the disc $|z| < \sqrt{2}$. Set

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

so that $P_n(x) - (x-1)P_{n-1}(x) + xP_{n-2}(x) = 0$ and $P_n(0) = (-1)^n Q(-2)$ for $n > k$. Then for every $n \geq k$, the roots of P_n and P_{n+1} are simple, contained in $[a, b]$, and interlaced.

In particular, if $Q(z) \in \mathbb{Z}[z]$, then $\{P_n\}$ is a good sequence. Note that $Q(z)(z+1)$ also satisfies the conditions and gives rise to the sequence $\{P_{n+1}\}$.

However, if we require $Q(-1) \neq 0$, then $\deg(Q) \leq 2\log_2 |Q(-2)|$. Hence for any fixed m, this construction yields only finitely many good sequences $\{P_n\}$ with $|P_n(0)| = m$.

A construction of sequences

Lemma (inspired by van Bommel–Costa–Poonen–Li–Smith)

Let $Q(z) := \sum_{i=0}^{k} a_i z^i$ be a monic real polynomial with all roots in the disc $|z| < \sqrt{2}$. Set

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

so that $P_n(x) - (x-1)P_{n-1}(x) + xP_{n-2}(x) = 0$ and $P_n(0) = (-1)^n Q(-2)$ for $n > k$. Then for every $n \geq k$, the roots of P_n and P_{n+1} are simple, contained in $[a, b]$, and interlaced.

In particular, if $Q(z) \in \mathbb{Z}[z]$, then $\{P_n\}$ is a good sequence. Note that $Q(z)(z+1)$ also satisfies the conditions and gives rise to the sequence $\{P_{n+1}\}$.

However, if we require $Q(-1) \neq 0$, then $\deg(Q) \leq 2\log_2 |Q(-2)|$. Hence for any fixed m, this construction yields only finitely many good sequences $\{P_n\}$ with $|P_n(0)| = m$.

A construction of sequences

Lemma (inspired by van Bommel–Costa–Poonen–Li–Smith)

Let $Q(z) := \sum_{i=0}^{k} a_i z^i$ be a monic real polynomial with all roots in the disc $|z| < \sqrt{2}$. Set

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

so that $P_n(x) - (x-1)P_{n-1}(x) + xP_{n-2}(x) = 0$ and $P_n(0) = (-1)^n Q(-2)$ for $n > k$. Then for every $n \geq k$, the roots of P_n and P_{n+1} are simple, contained in $[a, b]$, and interlaced.

In particular, if $Q(z) \in \mathbb{Z}[z]$, then $\{P_n\}$ is a good sequence. Note that $Q(z)(z+1)$ also satisfies the conditions and gives rise to the sequence $\{P_{n+1}\}$.

However, if we require $Q(-1) \neq 0$, then $\deg(Q) \leq 2\log_2 |Q(-2)|$. Hence for any fixed m, this construction yields only finitely many good sequences $\{P_n\}$ with $|P_n(0)| = m$.

Application of the construction

Every positive integer m admits a unique **nonadjacent binary representation** (Reitwiesner, 1960); i.e., there is a unique monic polynomial $Q(z)$ with $Q(2) = m$ with all coefficients in $\{-1, 0, 1\}$ and **no two consecutive** nonzero coefficients.

Lemma

If $Q(z)$ is the nonadjacent binary representation of some positive integer m, then $Q(z)$ has all roots in $|z| < \sqrt{2}$. Hence we may apply the previous lemma to $(-1)^{\deg(Q)} Q(-z)$ to produce a good sequence $\{P_n\}$ with $|P_n(0)| = m$.

As m grows, the number of good choices of Q grows. This will crucially give us some flexibility to impose alternate constraints, particularly on the mod-2 reduction. (This will however force us to handle some small m by hand-crafting a few good sequences.)

Application of the construction

Every positive integer m admits a unique **nonadjacent binary representation** (Reitwiesner, 1960); i.e., there is a unique monic polynomial $Q(z)$ with $Q(2) = m$ with all coefficients in $\{-1, 0, 1\}$ and **no two consecutive** nonzero coefficients.

Lemma

If $Q(z)$ is the nonadjacent binary representation of some positive integer m, then $Q(z)$ has all roots in $|z| < \sqrt{2}$. Hence we may apply the previous lemma to $(-1)^{\deg(Q)} Q(-z)$ to produce a good sequence $\{P_n\}$ with $|P_n(0)| = m$.

As m grows, the number of good choices of Q grows. This will crucially give us some flexibility to impose alternate constraints, particularly on the mod-2 reduction. (This will however force us to handle some small m by hand-crafting a few good sequences.)

Application of the construction

Every positive integer m admits a unique **nonadjacent binary representation** (Reitwiesner, 1960); i.e., there is a unique monic polynomial $Q(z)$ with $Q(2) = m$ with all coefficients in $\{-1, 0, 1\}$ and **no two consecutive** nonzero coefficients.

Lemma

If $Q(z)$ is the nonadjacent binary representation of some positive integer m, then $Q(z)$ has all roots in $|z| < \sqrt{2}$. Hence we may apply the previous lemma to $(-1)^{\deg(Q)} Q(-z)$ to produce a good sequence $\{P_n\}$ with $|P_n(0)| = m$.

As m grows, the number of good choices of Q grows. This will crucially give us some flexibility to impose alternate constraints, particularly on the mod-2 reduction. (This will however force us to handle some small m by hand-crafting a few good sequences.)

Contents

Overview

Theorem (Reminder of the statement we are trying to prove)

For any positive integer m, there exist infinitely many monic irreducible polynomials $R(T)$ with integer coefficients with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and $|R(0)| = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large degree.*

The case $m = 1$ was discussed earlier. For $m > 1$, we have at least one good sequence $P_n(x)$ with $|P_n(0)| = m$ for $n \gg 0$; however, these polynomials need not be irreducible!

We constrain the possible factorizations using three ingredients.

- A lemma of Skolem–Mahler–Lech type which limits the irreducible factors that arise in a single good sequence.
- Choosing good sequences with suitable mod-2 and 2-adic behavior, so that we can constrain the 2-adic Newton polygon of P_n for $n \gg 0$.
- When m is a power of an odd prime p, the p-adic Newton polygon.

Overview

Theorem (Reminder of the statement we are trying to prove)

For any positive integer m, there exist infinitely many monic irreducible polynomials $R(T)$ with integer coefficients with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and $|R(0)| = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large degree.*

The case $m = 1$ was discussed earlier. For $m > 1$, we have at least one good sequence $P_n(x)$ with $|P_n(0)| = m$ for $n \gg 0$; however, these polynomials need not be irreducible!

We constrain the possible factorizations using three ingredients.

- A lemma of Skolem–Mahler–Lech type which limits the irreducible factors that arise in a single good sequence.
- Choosing good sequences with suitable mod-2 and 2-adic behavior, so that we can constrain the 2-adic Newton polygon of P_n for $n \gg 0$.
- When m is a power of an odd prime p, the p-adic Newton polygon.

Overview

Theorem (Reminder of the statement we are trying to prove)

For any positive integer m, there exist infinitely many monic irreducible polynomials $R(T)$ with integer coefficients with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and $|R(0)| = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large degree.*

The case $m = 1$ was discussed earlier. For $m > 1$, we have at least one good sequence $P_n(x)$ with $|P_n(0)| = m$ for $n \gg 0$; however, these polynomials need not be irreducible!

We constrain the possible factorizations using three ingredients.

- A lemma of Skolem–Mahler–Lech type which limits the irreducible factors that arise in a single good sequence.
- Choosing good sequences with suitable mod-2 and 2-adic behavior, so that we can constrain the 2-adic Newton polygon of P_n for $n \gg 0$.
- When m is a power of an odd prime p, the p-adic Newton polygon.

Overview

Theorem (Reminder of the statement we are trying to prove)

For any positive integer m, there exist infinitely many monic irreducible polynomials $R(T)$ with integer coefficients with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and $|R(0)| = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large degree.*

The case $m = 1$ was discussed earlier. For $m > 1$, we have at least one good sequence $P_n(x)$ with $|P_n(0)| = m$ for $n \gg 0$; however, these polynomials need not be irreducible!

We constrain the possible factorizations using three ingredients.

- A lemma of Skolem–Mahler–Lech type which limits the irreducible factors that arise in a single good sequence.
- Choosing good sequences with suitable mod-2 and 2-adic behavior, so that we can constrain the 2-adic Newton polygon of P_n for $n \gg 0$.
- When m is a power of an odd prime p, the p-adic Newton polygon.

Overview

Theorem (Reminder of the statement we are trying to prove)

For any positive integer m, there exist infinitely many monic irreducible polynomials $R(T)$ with integer coefficients with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and $|R(0)| = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large degree.*

The case $m = 1$ was discussed earlier. For $m > 1$, we have at least one good sequence $P_n(x)$ with $|P_n(0)| = m$ for $n \gg 0$; however, these polynomials need not be irreducible!

We constrain the possible factorizations using three ingredients.

- A lemma of Skolem–Mahler–Lech type which limits the irreducible factors that arise in a single good sequence.
- Choosing good sequences with suitable mod-2 and 2-adic behavior, so that we can constrain the 2-adic Newton polygon of P_n for $n \gg 0$.
- When m is a power of an odd prime p, the p-adic Newton polygon.

Overview

Theorem (Reminder of the statement we are trying to prove)

For any positive integer m, there exist infinitely many monic irreducible polynomials $R(T)$ with integer coefficients with all roots in $[a, b] = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and $|R(0)| = m$. Moreover, when m is even or a power of an odd prime, these exist in **every** *sufficiently large degree.*

The case $m = 1$ was discussed earlier. For $m > 1$, we have at least one good sequence $P_n(x)$ with $|P_n(0)| = m$ for $n \gg 0$; however, these polynomials need not be irreducible!

We constrain the possible factorizations using three ingredients.

- A lemma of Skolem–Mahler–Lech type which limits the irreducible factors that arise in a single good sequence.
- Choosing good sequences with suitable mod-2 and 2-adic behavior, so that we can constrain the 2-adic Newton polygon of P_n for $n \gg 0$.
- When m is a power of an odd prime p, the p-adic Newton polygon.

A lemma of Skolem–Mahler–Lech type

Lemma

Let $\{P_n(x)\}$ be a sequence of monic integer polynomials satisfying

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

Suppose for some $n' < n$, $P_n(x)$ and $P_{n'}(x)$ have a nontrivial common factor $Q(x)$ which does not divide **every** *term in the sequence. Then $|Q(0)| = 1$ and $Q(x)$ divides $P_{n+k(n'-n)}$ for all k.*

We apply this as follows. Suppose that for some $n \gg 0$, P_n admits a "big" irreducible factor, i.e., one whose cofactor has degree bounded independently of n. Then this cofactor eventually has constant term ± 1: there are only finitely many other options and each can occur only once. Hence removing the cofactor gives an irreducible polynomial $Q(x)$ with $|Q(0)| = |P_n(0)|$.

A lemma of Skolem–Mahler–Lech type

Lemma

Let $\{P_n(x)\}$ be a sequence of monic integer polynomials satisfying

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

Suppose for some $n' < n$, $P_n(x)$ and $P_{n'}(x)$ have a nontrivial common factor $Q(x)$ which does not divide **every** *term in the sequence. Then $|Q(0)| = 1$ and $Q(x)$ divides $P_{n+k(n'-n)}$ for all k.*

We apply this as follows. Suppose that for some $n \gg 0$, P_n admits a "big" irreducible factor, i.e., one whose cofactor has degree bounded independently of n. Then this cofactor eventually has constant term ± 1: there are only finitely many other options and each can occur only once. Hence removing the cofactor gives an irreducible polynomial $Q(x)$ with $|Q(0)| = |P_n(0)|$.

Modified nonadjacent binary representations

As indicated earlier, the construction of good sequences using nonadjacent binary representations leaves a bit of wiggle room to adjust the seed polynomial.

Lemma

For every positive integer $m \notin \{4, 8, 20\}$, there exists a monic integer polynomial $Q(z)$ with:

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

(In the paper we call this a **compliant representation** *of* m*.)*

Key idea of the proof: add a restriction on $\min\{|Q(z)| : |z| \leq \sqrt{2}\}$, then recurse via $Q(z) \mapsto (z^4 - 1)Q(z) + k$ (using many base cases found by computer).

Modified nonadjacent binary representations

As indicated earlier, the construction of good sequences using nonadjacent binary representations leaves a bit of wiggle room to adjust the seed polynomial.

Lemma

For every positive integer $m \notin \{4, 8, 20\}$, there exists a monic integer polynomial $Q(z)$ with:

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

(In the paper we call this a **compliant representation** *of* m*.)*

Key idea of the proof: add a restriction on $\min\{|Q(z)| : |z| \leq \sqrt{2}\}$, then recurse via $Q(z) \mapsto (z^4 - 1)Q(z) + k$ (using many base cases found by computer).

Modified nonadjacent binary representations

As indicated earlier, the construction of good sequences using nonadjacent binary representations leaves a bit of wiggle room to adjust the seed polynomial.

Lemma

For every positive integer $m \notin \{4, 8, 20\}$, there exists a monic integer polynomial $Q(z)$ with:

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

(In the paper we call this a **compliant representation** *of m.)*

Key idea of the proof: add a restriction on $\min\{|Q(z)| : |z| \leq \sqrt{2}\}$, then recurse via $Q(z) \mapsto (z^4 - 1)Q(z) + k$ (using many base cases found by computer).

Modified nonadjacent binary representations

As indicated earlier, the construction of good sequences using nonadjacent binary representations leaves a bit of wiggle room to adjust the seed polynomial.

Lemma

For every positive integer $m \notin \{4, 8, 20\}$, there exists a monic integer polynomial $Q(z)$ with:

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

(In the paper we call this a **compliant representation** *of* m*.)*

Key idea of the proof: add a restriction on $\min\{|Q(z)| : |z| \leq \sqrt{2}\}$, then recurse via $Q(z) \mapsto (z^4 - 1)Q(z) + k$ (using many base cases found by computer).

Modified nonadjacent binary representations

As indicated earlier, the construction of good sequences using nonadjacent binary representations leaves a bit of wiggle room to adjust the seed polynomial.

Lemma

For every positive integer $m \notin \{4, 8, 20\}$, there exists a monic integer polynomial $Q(z)$ with:

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

(In the paper we call this a **compliant representation** *of* m*.)*

Key idea of the proof: add a restriction on $\min\{|Q(z)| : |z| \leq \sqrt{2}\}$, then recurse via $Q(z) \mapsto (z^4 - 1)Q(z) + k$ (using many base cases found by computer).

Modified nonadjacent binary representations

As indicated earlier, the construction of good sequences using nonadjacent binary representations leaves a bit of wiggle room to adjust the seed polynomial.

Lemma

For every positive integer $m \notin \{4, 8, 20\}$, there exists a monic integer polynomial $Q(z)$ with:

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

(In the paper we call this a **compliant representation** *of* m*.)*

Key idea of the proof: add a restriction on $\min\{|Q(z)| : |z| \leq \sqrt{2}\}$, then recurse via $Q(z) \mapsto (z^4 - 1)Q(z) + k$ (using many base cases found by computer).

The case of m even

Remember that every good sequence has mod-2 reductions of the form $A + Bx^n$. For m even, starting with a compliant representation of m gives

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

By computing $P_n(x) \pmod{(4, x^2)}$, we see that P_n has 2-adic Newton slopes

$$\begin{cases} 0, \frac{1}{n-1} \times (n-1) & m \equiv 2 \pmod 4 \\ 0, \frac{1}{n-2} \times (n-2), v_2(m) - 1 & m \equiv 0 \pmod 4. \end{cases}$$

If P_n is reducible, it has an irreducible factor of degree ≤ 2. For $n \gg 0$, the common factors lemma shows that this factor must be $x - 1$, which is impossible because $P_n(1) \equiv 2 \pmod 4$.

For $m = 4, 8, 20$, we directly find initial terms P_0, P_1 giving a good sequence with $|P_n(0)| = m$.

The case of m even

Remember that every good sequence has mod-2 reductions of the form $A + Bx^n$. For m even, starting with a compliant representation of m gives

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

By computing $P_n(x) \pmod{(4, x^2)}$, we see that P_n has 2-adic Newton slopes

$$\begin{cases} 0, \frac{1}{n-1} \times (n-1) & m \equiv 2 \pmod 4 \\ 0, \frac{1}{n-2} \times (n-2), v_2(m) - 1 & m \equiv 0 \pmod 4. \end{cases}$$

If P_n is reducible, it has an irreducible factor of degree ≤ 2. For $n \gg 0$, the common factors lemma shows that this factor must be $x - 1$, which is impossible because $P_n(1) \equiv 2 \pmod 4$.

For $m = 4, 8, 20$, we directly find initial terms P_0, P_1 giving a good sequence with $|P_n(0)| = m$.

The case of m even

Remember that every good sequence has mod-2 reductions of the form $A + Bx^n$. For m even, starting with a compliant representation of m gives

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

By computing $P_n(x) \pmod{(4, x^2)}$, we see that P_n has 2-adic Newton slopes

$$\begin{cases} 0, \frac{1}{n-1} \times (n-1) & m \equiv 2 \pmod 4 \\ 0, \frac{1}{n-2} \times (n-2), v_2(m) - 1 & m \equiv 0 \pmod 4. \end{cases}$$

If P_n is reducible, it has an irreducible factor of degree ≤ 2. For $n \gg 0$, the common factors lemma shows that this factor must be $x - 1$, which is impossible because $P_n(1) \equiv 2 \pmod 4$.

For $m = 4, 8, 20$, we directly find initial terms P_0, P_1 giving a good sequence with $|P_n(0)| = m$.

The case of m even

Remember that every good sequence has mod-2 reductions of the form $A + Bx^n$. For m even, starting with a compliant representation of m gives

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

By computing $P_n(x) \pmod{(4, x^2)}$, we see that P_n has 2-adic Newton slopes

$$\begin{cases} 0, \frac{1}{n-1} \times (n-1) & m \equiv 2 \pmod 4 \\ 0, \frac{1}{n-2} \times (n-2), v_2(m) - 1 & m \equiv 0 \pmod 4. \end{cases}$$

If P_n is reducible, it has an irreducible factor of degree ≤ 2. For $n \gg 0$, the common factors lemma shows that this factor must be $x - 1$, which is impossible because $P_n(1) \equiv 2 \pmod 4$.

For $m = 4, 8, 20$, we directly find initial terms P_0, P_1 giving a good sequence with $|P_n(0)| = m$.

The case of m odd

For m odd, the compliant representation gives $P_n(x) \equiv x^n + 1 \pmod 2$ and $P_n(1) \equiv 2 \pmod 4$. When n is a power of 2, $P_n(x+1)$ is Eisenstein at 2; we deduce irreducibility for infinitely many n, but not $n \gg 0$.

For m a power of an odd prime p, we can also use p-adic slopes. If $P_n'(0) \not\equiv 0 \pmod p$, then the p-adic Newton slopes are $0 \times (n-1), v_p(m)$; if P_n is reducible, it has an irreducible factor $Q(x)$ with $Q(0) \not\equiv 0 \pmod p$ and hence $|Q(0)| = \pm 1$.

It will thus suffice to prove the following.

Theorem

For $m > 1$ odd, there exists a good sequence $\{P_n\}$ with $|P_n(0)| = m$ such that for $n \gg 0$, P_n has no irreducible factor Q with $|Q(0)| = \pm 1$. When m is a power of a prime p, we can further ensure that $P_n'(0) \not\equiv 0 \pmod p$.

The case of m odd

For m odd, the compliant representation gives $P_n(x) \equiv x^n + 1 \pmod 2$ and $P_n(1) \equiv 2 \pmod 4$. When n is a power of 2, $P_n(x+1)$ is Eisenstein at 2; we deduce irreducibility for infinitely many n, but not $n \gg 0$.

For m a power of an odd prime p, we can also use p-adic slopes. If $P_n'(0) \not\equiv 0 \pmod p$, then the p-adic Newton slopes are $0 \times (n-1), v_p(m)$; if P_n is reducible, it has an irreducible factor $Q(x)$ with $Q(0) \not\equiv 0 \pmod p$ and hence $|Q(0)| = \pm 1$.

It will thus suffice to prove the following.

Theorem

For $m > 1$ odd, there exists a good sequence $\{P_n\}$ with $|P_n(0)| = m$ such that for $n \gg 0$, P_n has no irreducible factor Q with $|Q(0)| = \pm 1$. When m is a power of a prime p, we can further ensure that $P_n'(0) \not\equiv 0 \pmod p$.

The case of m odd (continued)

Theorem

For $m > 1$ odd, there exists a good sequence $\{P_n\}$ with $|P_n(0)| = m$ such that for $n \gg 0$, P_n has no irreducible factor Q with $|Q(0)| = \pm 1$.

To prove this, we modify the definition of a compliant representation to enforce

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

Now we take advantage of the Madan–Pal classification: if Q is an irreducible factor of P_n with $|Q(0)| = \pm 1$, then Q is derived from a cyclotomic polynomial $\Phi_k(x)$ and the mod-2 reduction of $\Phi_k(x)$ divides $x^n + x^{n-1} + x^{n-2} + 1$ only for small k.

This leaves a small (uniform in m) number of possible factors Q. However, for $m \gg 0$ we arrange to obtain a handful of good sequences such that each Q can only occur as a recurring (by the common factors lemma) factor for at most one of our sequences.

The case of m odd (continued)

Theorem

For $m > 1$ odd, there exists a good sequence $\{P_n\}$ with $|P_n(0)| = m$ such that for $n \gg 0$, P_n has no irreducible factor Q with $|Q(0)| = \pm 1$.

To prove this, we modify the definition of a compliant representation to enforce

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

Now we take advantage of the Madan–Pal classification: if Q is an irreducible factor of P_n with $|Q(0)| = \pm 1$, then Q is derived from a cyclotomic polynomial $\Phi_k(x)$ and the mod-2 reduction of $\Phi_k(x)$ divides $x^n + x^{n-1} + x^{n-2} + 1$ only for small k.

This leaves a small (uniform in m) number of possible factors Q. However, for $m \gg 0$ we arrange to obtain a handful of good sequences such that each Q can only occur as a recurring (by the common factors lemma) factor for at most one of our sequences.

The case of m odd (continued)

Theorem

For $m > 1$ odd, there exists a good sequence $\{P_n\}$ with $|P_n(0)| = m$ such that for $n \gg 0$, P_n has no irreducible factor Q with $|Q(0)| = \pm 1$.

To prove this, we modify the definition of a compliant representation to enforce

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

Now we take advantage of the Madan–Pal classification: if Q is an irreducible factor of P_n with $|Q(0)| = \pm 1$, then Q is derived from a cyclotomic polynomial $\Phi_k(x)$ and the mod-2 reduction of $\Phi_k(x)$ divides $x^n + x^{n-1} + x^{n-2} + 1$ only for small k.

This leaves a small (uniform in m) number of possible factors Q. However, for $m \gg 0$ we arrange to obtain a handful of good sequences such that each Q can only occur as a recurring (by the common factors lemma) factor for at most one of our sequences.

The case of m odd (continued)

Theorem

For $m > 1$ odd, there exists a good sequence $\{P_n\}$ with $|P_n(0)| = m$ such that for $n \gg 0$, P_n has no irreducible factor Q with $|Q(0)| = \pm 1$.

To prove this, we modify the definition of a compliant representation to enforce

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

Now we take advantage of the Madan–Pal classification: if Q is an irreducible factor of P_n with $|Q(0)| = \pm 1$, then Q is derived from a cyclotomic polynomial $\Phi_k(x)$ and the mod-2 reduction of $\Phi_k(x)$ divides $x^n + x^{n-1} + x^{n-2} + 1$ only for small k.

This leaves a small (uniform in m) number of possible factors Q. However, for $m \gg 0$ we arrange to obtain a handful of good sequences such that each Q can only occur as a recurring (by the common factors lemma) factor for at most one of our sequences.

Contents

What really should be true

Conjecture

Let $f(g, m)$ denote the number of isogeny classes of simple abelian varieties over $\mathbb{F}_2$ of dimension g and order m. Then for fixed m, $f(g, m) \to \infty$ as $g \to \infty$.

Some evidence: if one picks P_n, P_{n+1} of degrees $n, n+1$ with all roots simple in $[a, b]$ (but not necessarily interlaced), these "often" generate a good sequence.

Instead of simple abelian varieties, we might consider abelian varieties having no isogeny factor of order 1. This should not appreciably affect the asymptotics but might make the analysis easier.

What really should be true

Conjecture

Let $f(g, m)$ denote the number of isogeny classes of simple abelian varieties over $\mathbb{F}_2$ of dimension g and order m. Then for fixed m, $f(g, m) \to \infty$ as $g \to \infty$.

Some evidence: if one picks P_n, P_{n+1} of degrees $n, n+1$ with all roots simple in $[a, b]$ (but not necessarily interlaced), these "often" generate a good sequence.

Instead of simple abelian varieties, we might consider abelian varieties having no isogeny factor of order 1. This should not appreciably affect the asymptotics but might make the analysis easier.

What really should be true

Conjecture

Let $f(g, m)$ denote the number of isogeny classes of simple abelian varieties over $\mathbb{F}_2$ of dimension g and order m. Then for fixed m, $f(g, m) \to \infty$ as $g \to \infty$.

Some evidence: if one picks P_n, P_{n+1} of degrees $n, n+1$ with all roots simple in $[a, b]$ (but not necessarily interlaced), these "often" generate a good sequence.

Instead of simple abelian varieties, we might consider abelian varieties having no isogeny factor of order 1. This should not appreciably affect the asymptotics but might make the analysis easier.

A bit of numerical evidence

Conjecture

Let $f(g, m)$ denote the number of isogeny classes of abelian varieties over $\mathbb{F}_2$ of dimension g and order m. Then for fixed m, $f(g, m) \to \infty$ as $g \to \infty$.

Using my code for computing Weil polynomials in SageMath, I computed:

g	1	2	3	4	5	6	7	8	9	10	11
$f(g, 2)$	1	3	4	10	9	28	24	54	50	86	63

Does this suggest anything about the asymptotic growth of $f(g, m)$ for fixed m? If so, please let me know...

A bit of numerical evidence

Conjecture

Let $f(g, m)$ denote the number of isogeny classes of abelian varieties over $\mathbb{F}_2$ of dimension g and order m. Then for fixed m, $f(g, m) \to \infty$ as $g \to \infty$.

Using my code for computing Weil polynomials in SageMath, I computed:

g	1	2	3	4	5	6	7	8	9	10	11
$f(g, 2)$	1	3	4	10	9	28	24	54	50	86	63

Does this suggest anything about the asymptotic growth of $f(g, m)$ for fixed m? If so, please let me know...

Contents

References (and the QR code for these slides again)

K.S. Kedlaya, Abelian varieties over $\mathbb{F}_2$ of prescribed order [arXiv, DOI].
K.S. Kedlaya, Abelian varieties over $\mathbb{F}_2$ of prescribed order and dimension [preprint].