Weil polynomials of abelian varieties over finite fields with many rational points

Elena Berardini[1] & A. J. Giangreco–Maidana[2]

1. Eindhoven University of Technology
2. Universidad Nacional de Asunción

DIAMANT Symposium Autumn 2022

Elena Berardini has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 899987.

Main characters of the talk

$\mathcal{I}^0_{\max}(g,q)$ the maximal simple and ordinary isogeny class of abelian varieties of dimension g, defined over $\mathbb{F}_q$.

Main characters of the talk

$\mathcal{I}^0_{\max}(g,q)$ the maximal simple and ordinary isogeny class of abelian varieties of dimension g, defined over $\mathbb{F}_q$.

Maximality: maximal number of rational points.

Main characters of the talk

$\mathcal{I}^0_{\max}(g,q)$ the maximal simple and ordinary isogeny class of abelian varieties of dimension g, defined over $\mathbb{F}_q$.

Maximality: maximal number of rational points.

$\mathfrak{f}_g$ the minimal polynomial of an algebraic totally positive integer of degree g with minimal trace and which is "maximal".

Main characters of the talk

$\mathcal{I}^0_{\max}(g,q)$ the maximal simple and ordinary isogeny class of abelian varieties of dimension g, defined over $\mathbb{F}_q$.

Maximality: maximal number of rational points.

$\mathfrak{f}_g$ the minimal polynomial of an algebraic totally positive integer of degree g with minimal trace and which is "maximal".

Maximality: under a certain order relation (defined later).

Spoiler

Theorem (B., Giangreco '22)

Let g be an positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is an even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g, q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t, X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

Spoiler

Theorem (B., Giangreco '22)

Let g be an positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is an even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g,q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t,X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

Corollary (B., Giangreco '22)

$\mathcal{I}^0_{max}(g,q)$ is ℓ-cyclic for all prime numbers ℓ that do not divide

$$N_g := \mathfrak{f}_g(4)\mathfrak{f}_g(0)\Delta_g,$$

where Δ_g is the discriminant of $\mathfrak{f}_g$.

Some motivations

Weil polynomials are a fundamental tool to study isogeny classes of abelian varieties

Some motivations

Weil polynomials are a fundamental tool to study isogeny classes of abelian varieties

$\rightarrow$ precise criteria for determining if a polynomial is the Weil polynomial of an isogeny class are known only in "small" dimension (Deuring, Waterhouse, Rück, Xing, Haloui,...)

Some motivations

Weil polynomials are a fundamental tool to study isogeny classes of abelian varieties

$\rightarrow$ precise criteria for determining if a polynomial is the Weil polynomial of an isogeny class are known only in "small" dimension (Deuring, Waterhouse, Rück, Xing, Haloui,...)

Abelian varieties and their groups of rational points intervene in cryptography and geometric coding theory

Abelian varieties: first step

Definition

An abelian variety A defined over a field k is a connected and completed variety with a group structure over $A(\bar{k})$. It is called simple if it does not contain proper abelian sub-varieties $\neq 0$.

Example: elliptic curves are abelian varieties of dimension 1.

Abelian varieties: first step

Definition

An abelian variety A defined over a field k is a connected and completed variety with a group structure over $A(\bar{k})$. It is called simple if it does not contain proper abelian sub-varieties $\neq 0$.

Example: elliptic curves are abelian varieties of dimension 1.

Definition

An isogeny is a surjective homomorphism from A to B with $\dim(A) = \dim(B)$. An isogeny from A to B implies the existence of an isogeny from B to A. This defines an equivalence relation. We say that A and B are isogenous, $A \sim B$. We denote $\mathcal{A}$ an isogeny class.

Abelian varieties: first step

Definition

An abelian variety A defined over a field k is a connected and completed variety with a group structure over $A(\bar{k})$. It is called simple if it does not contain proper abelian sub-varieties $\neq 0$.

Example: elliptic curves are abelian varieties of dimension 1.

Definition

An isogeny is a surjective homomorphism from A to B with $\dim(A) = \dim(B)$. An isogeny from A to B implies the existence of an isogeny from B to A. This defines an equivalence relation. We say that A and B are isogenous, $A \sim B$. We denote $\mathcal{A}$ an isogeny class.

Theorem (Poincaré Splitting Theorem)

An abelian variety A defined over a field k is (uniquely) isogenous to the product

$$A \sim B_1^{e_1} \times \cdots \times B_n^{e_n}$$

where the abelian varieties B_i are simple and pairwise non isogenous over k.

Abelian varieties: second step

$f_A(t)$: the characteristic polynomial of the Frobenius endomorphism

Multiplication map:

$$m_A : A \to A$$
$$P \mapsto mP$$

p-rank and ordinary varieties:
Let $q = p^r$, we define

$$A[p](\overline{\mathbb{F}}_q) := \ker(p_A).$$

We call the p-rank of A the dimension of $A[p](\overline{\mathbb{F}}_q)$.

Definition

An abelian variety with maximal p-rank is called ordinary.

Weil polynomials

Definition

Let $q = p^r$. A Weil q-polynomial is a monic even degree polynomial with integer coefficients, whose all roots are algebraic integers of absolute value $\sqrt{q}$. Over the real numbers, it is of the form

$$\prod_i (t^2 + x_i t + q), \quad x_i \in \mathbb{R} \text{ and } |x_i| \leq 2\sqrt{q}.$$

It is called ordinary if the middle coefficient is not divisible by p.

Weil polynomials

Definition

Let $q = p^r$. A Weil q-polynomial is a monic even degree polynomial with integer coefficients, whose all roots are algebraic integers of absolute value $\sqrt{q}$. Over the real numbers, it is of the form

$$\prod_i (t^2 + x_i t + q), \quad x_i \in \mathbb{R} \text{ and } |x_i| \leq 2\sqrt{q}.$$

It is called ordinary if the middle coefficient is not divisible by p.

Weil: $f_A(t)$ is a Weil q-polynomial

Tate: $A \sim B \iff f_A(t) = f_B(t)$

Weil polynomials

Definition

Let $q = p^r$. A Weil q-polynomial is a monic even degree polynomial with integer coefficients, whose all roots are algebraic integers of absolute value $\sqrt{q}$. Over the real numbers, it is of the form

$$\prod_i (t^2 + x_i t + q), \quad x_i \in \mathbb{R} \text{ and } |x_i| \leq 2\sqrt{q}.$$

It is called ordinary if the middle coefficient is not divisible by p.

Weil: $f_A(t)$ is a Weil q-polynomial

Tate: $A \sim B \iff f_A(t) = f_B(t)$

Hence, we can talk about the Weil polynomial of an isogeny class $\mathcal{A}$:

$$f_{\mathcal{A}}(t)$$

Classical and ordinary Honda–Tate theory

Honda–Tate theory

$$\left\{\begin{array}{c}\textit{isogeny classes of simple abelian}\\ \textit{varieties defined over } \mathbb{F}_q\end{array}\right\} \iff \{\textit{irreducible Weil } q\textit{-polynomials}\}$$

⚠ not all irreducible Weil q-polynomials are Weil polynomials of a simple isogeny class;
⚠ not all simple isogeny classes have an irreducible Weil polynomial.

Classical and ordinary Honda–Tate theory

Honda–Tate theory

$$\left\{\begin{array}{c}\textit{isogeny classes of simple abelian}\\ \textit{varieties defined over } \mathbb{F}_q\end{array}\right\} \iff \{\textit{irreducible Weil } q\textit{-polynomials}\}$$

⚠ not all irreducible Weil q-polynomials are Weil polynomials of a simple isogeny class;
⚠ not all simple isogeny classes have an irreducible Weil polynomial.

✔ The Weil polynomial of a simple isogeny class is

$$f_{\mathcal{A}}(t) = h(t)^e,$$

for $h(t) \in \mathbb{Z}[t]$ an irreducible q-polynomial and e a positive integer.

Classical and ordinary Honda–Tate theory

Honda–Tate theory

$$\left\{\begin{array}{c}\textit{isogeny classes of simple abelian}\\ \textit{varieties defined over } \mathbb{F}_q\end{array}\right\} \iff \left\{\textit{irreducible Weil } q\textit{-polynomials}\right\}$$

⚠ not all irreducible Weil q-polynomials are Weil polynomials of a simple isogeny class;
⚠ not all simple isogeny classes have an irreducible Weil polynomial.

✔ The Weil polynomial of a simple isogeny class is

$$f_{\mathcal{A}}(t) = h(t)^e,$$

for $h(t) \in \mathbb{Z}[t]$ an irreducible q-polynomial and e a positive integer.

Honda–Tate theory (Ordinary)

An ordinary and irreducible Weil q-polynomial is always the Weil polynomial of a simple ordinary isogeny class.

What information do we get from the Weil polynomial?

The cardinality of the group of rational points:

$$\#A(\mathbb{F}_q) = f_A(1)$$

The property of being ordinary:

$$\mathcal{A} \text{ is ordinary} \iff f_{\mathcal{A}}(t) \text{ is an ordinary Weil } q\text{-polynomial}$$

The cyclicity of the group of rational points[1]: for a prime number ℓ we have

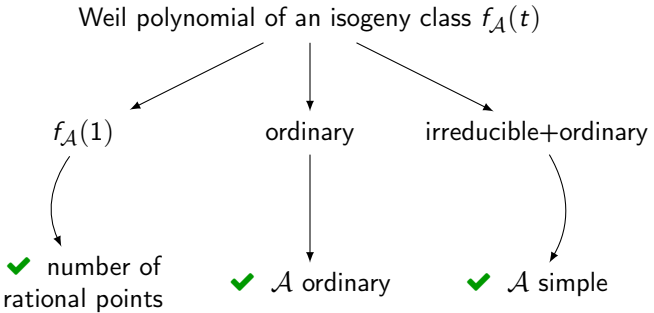
$$\mathcal{A} \text{ is } \ell\text{-cyclic} \iff \ell \text{ does not divide } (\widehat{f_{\mathcal{A}}(1)}, f'_{\mathcal{A}}(1)),$$

where:

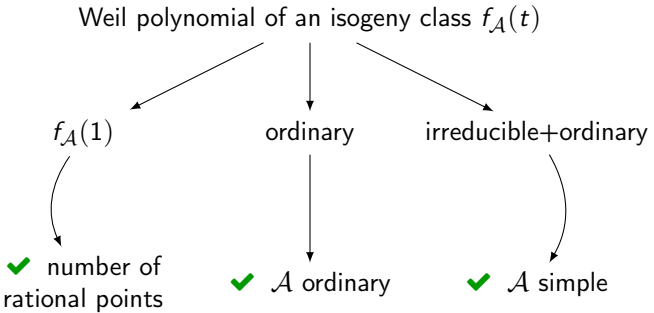
- an isogeny class $\mathcal{A}$ is called ℓ-cyclic if $A(\mathbb{F}_q)_\ell$ is cyclic for any $A \in \mathcal{A}$, $A(\mathbb{F}_q)_\ell$ being the ℓ-part of the group of rational points of A;
- for an integer z, $\widehat{z}$ denotes the quotient of z by its radical.

[1] A. Giangreco–Maidana, Finite Fields Appl., 57 (2019).

So far, so good?



So far, so good?



✔ cyclicity criterion for isogeny classes

Algebraic integers enter the game

Definition

An algebraic integer is a complex number that is the root of a monic polynomial with coefficients in $\mathbb{Z}$. It is called totally positive if all its conjugates are positive real numbers.

Ann. Inst. Fourier, Grenoble
33, 3 (1984), 1-28

TOTALLY POSITIVE ALGEBRAIC INTEGERS OF SMALL TRACE

by Christopher SMYTH

Let $r \geqslant 0$ be a given integer. We describe an algorithm for finding all totally positive algebraic integers α which satisfy

$$\mathrm{Tr}\,\alpha - \deg\alpha = r \qquad (1)$$

(where $\mathrm{Tr}\,\alpha$ = trace of α, $\deg\alpha$ = degree of α). That r must be non-negative is an immediate consequence of the inequality of the arithmetic and geometric means. The algorithm is based on a recent improvement [5] of a result of Siegel [3], combined with a method of Robinson [1] for enumerating totally real polynomials of a specific type. The algorithm was implemented on the University College, Cardiff, Honeywell computer which took 40 minutes CPU time to find all relevant α with $r = 0, 1, 2, \ldots, 6$. (Almost all of this time was spent on the last case: $r = 6$, $\deg\alpha = 7$). The table of these α appears as an appendix to this paper.

This work was stimulated by a question of Serre, who asked for a list of these algebraic integers, for an application connected with bounding the number of points on algebraic curves over finite fields.

Minimal polynomials of algebraic integers

$\mathcal{F}_g$: the set of minimal polynomial of totally positive algebraic integers of degree g;

that is

the set of monic polynomials of degree g with integer coefficients, irreducible over $\mathbb{Q}$ and whose roots are positive real numbers.

$\mathcal{F}_g^{\min}$: the subset of $\mathcal{F}_g$ of minimal trace polynomials.

Minimal polynomials of algebraic integers

$\mathcal{F}_g$: the set of minimal polynomial of totally positive algebraic integers of degree g;

that is

the set of monic polynomials of degree g with integer coefficients, irreducible over $\mathbb{Q}$ and whose roots are positive real numbers.

$\mathcal{F}_g^{\min}$: the subset of $\mathcal{F}_g$ of minimal trace polynomials.

Lemma (B., Giangreco '22)

Let g be a positive integer. There exists a polynomial $\mathfrak{f}_g \in \mathcal{F}_g^{\min}$ and a real number n_g such that $\mathfrak{f}_g(t) > f(t)$ for any other polynomial $f \in \mathcal{F}_g$ and $t > n_g$.

In particular, $\mathfrak{f}_g$ is the maximal element of $\mathcal{F}_g^{\min}$ under the order relation:

$$f_1 \leq f_2 \iff f_2 - f_1 \text{ has non-negative leading coefficient.}$$

Main theorem: sketch of the proof

Theorem (B., Giangreco '22)

Let g be a positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is the even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g, q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t, X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

Main theorem: sketch of the proof

Theorem (B., Giangreco '22)

Let g be a positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is the even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g, q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t, X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

1. show that $h_g(t, \sqrt{q})$ is a Weil q-polynomial

Main theorem: sketch of the proof

Theorem (B., Giangreco '22)

Let g be a positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is the even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g, q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t, X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

1. show that $h_g(t, \sqrt{q})$ is a Weil q-polynomial, ordinary

Main theorem: sketch of the proof

Theorem (B., Giangreco '22)

Let g be a positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is the even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g, q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t, X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

1. show that $h_g(t, \sqrt{q})$ is a Weil q-polynomial, ordinary, irreducible over $\mathbb{Q}$;

Main theorem: sketch of the proof

Theorem (B., Giangreco '22)

Let g be a positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is the even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g, q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t, X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

1. show that $h_g(t, \sqrt{q})$ is a Weil q-polynomial, ordinary, irreducible over $\mathbb{Q}$;
2. apply ordinary Honda–Tate theory $\Rightarrow$ $h_g(t, \sqrt{q})$ is the Weil polynomial of a simple ordinary isogeny class;

Main theorem: sketch of the proof

Theorem (B., Giangreco '22)

Let g be a positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is the even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g, q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t, X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

1. show that $h_g(t, \sqrt{q})$ is a Weil q-polynomial, ordinary, irreducible over $\mathbb{Q}$;
2. apply ordinary Honda–Tate theory $\Rightarrow$ $h_g(t, \sqrt{q})$ is the Weil polynomial of a simple ordinary isogeny class;
3. $\#\mathcal{I}^0_{\mathrm{max}}(g, q)(\mathbb{F}_q) = h_g(1, \sqrt{q}) = \mathfrak{f}_g((\sqrt{q} + 1)^2)$;

Main theorem: sketch of the proof

Theorem (B., Giangreco '22)

Let g be a positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is the even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g, q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t, X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

1. show that $h_g(t, \sqrt{q})$ is a Weil q-polynomial, ordinary, irreducible over $\mathbb{Q}$;
2. apply ordinary Honda–Tate theory $\Rightarrow$ $h_g(t, \sqrt{q})$ is the Weil polynomial of a simple ordinary isogeny class;
3. $\#\mathcal{I}^0_{\max}(g, q)(\mathbb{F}_q) = h_g(1, \sqrt{q}) = \mathfrak{f}_g((\sqrt{q} + 1)^2)$;
4. maximality of $\mathfrak{f}_g \Rightarrow$ maximality of $\mathcal{I}^0_{\max}(g, q)$ within simple ordinary isogeny classes.

Main theorem: sketch of the proof

Theorem (B., Giangreco '22)

Let g be a positive integer and let $r_1, \dots, r_g$ be the roots of the polynomial $\mathfrak{f}_g$. Then, there exists a real number c_g such that for any $q = p^{2e} > c_g$ (q is the even power of a prime p), coprime with $\mathfrak{f}_g(0)$, the isogeny class $\mathcal{I}^0_{max}(g,q)$ exists and has Weil polynomial $h_g(t, \sqrt{q})$, where

$$h_g(t,X) := \prod_{i=1}^{g} (t^2 + (2X - r_i)t + X^2).$$

Corollary (B., Giangreco '22)

$\mathcal{I}^0_{max}(g,q)$ is ℓ-cyclic for all prime numbers ℓ that do not divide

$$N_g := \mathfrak{f}_g(4)\mathfrak{f}_g(0)\Delta_g,$$

where Δ_g is the discriminant of $\mathfrak{f}_g$.

Take away

knowledge of $\mathfrak{f}_g$ $\iff$ knowledge of the Weil polynomial of $\mathcal{I}^0_{\max}(g,q)$ + cyclicity

Take away

knowledge of $\mathfrak{f}_g$ $\iff$ knowledge of the Weil polynomial of $\mathcal{I}^0_{\max}(g,q)$ + cyclicity

When the set $\mathcal{F}_g^{\min}$ is known, we deduce $\mathfrak{f}_g$, hence N_g. Some examples[2]:

$\mathfrak{f}_g(t)$	$\mathfrak{f}_g(4)$	$\mathfrak{f}_g(0)$	Δ_g
$t-1$	3	-1	1
t^2-3t+1	5	1	5
t^3-5t^2+6t-1	7	-1	7^2
$t^4-7t^3+14t^2-8t+1$	1	1	$3^2\times 5^3$
$t^5-9t^4+28t^3-35t^2+15t-1$	11	-1	11^4
$t^6-11t^5+45t^4-84t^3+70t^2-21t+1$	13	1	13^5

[2] C. J. Smyth, Ann. Inst. Fourier Grenoble, 34, 1984

Further research

1. What can we say when q is an odd power of a prime?
   - $\rightarrow$ Is there a polynomial "parametrising" $\mathcal{I}^0_{\max}(g, q)$?
   - $\rightarrow$ Are there arbitrarily large prime numbers ℓ such that $\mathcal{I}^0_{\max}(g, q)$ is not ℓ-cyclic for some odd power q?

Further research

1. What can we say when q is an odd power of a prime?
   - $\rightarrow$ Is there a polynomial "parametrising" $\mathcal{I}^0_{\max}(g,q)$?
   - $\rightarrow$ Are there arbitrarily large prime numbers ℓ such that $\mathcal{I}^0_{\max}(g,q)$ is not ℓ-cyclic for some odd power q?

2. maximal simple ordinary isogeny class $\overset{?}{\Leftrightarrow}$ maximal simple ~~ordinary~~ isogeny class

Further research

1. What can we say when q is an odd power of a prime?
   - $\rightarrow$ Is there a polynomial "parametrising" $\mathcal{I}^0_{\max}(g, q)$?
   - $\rightarrow$ Are there arbitrarily large prime numbers ℓ such that $\mathcal{I}^0_{\max}(g, q)$ is not ℓ-cyclic for some odd power q?

2. maximal simple ordinary isogeny class $\overset{?}{\Leftrightarrow}$ maximal simple ~~ordinary~~ isogeny class
   - $\rightarrow$ The maximal simple isogeny class always has a irreducible Weil polynomial?

Thank you for your attention!

Questions?

e.berardini@tue.nl
agiangreco@ing.una.py