Abelian varieties of prescribed order

Raymond van Bommel

Massachusetts Institute of Technology

Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation

These slides can be downloaded at

`raymondvanbommel.nl/talks/linfoot.pdf`

Massachusetts Institute of Technology

Abelian varieties of prescribed order

Raymond van Bommel

Massachusetts Institute of Technology
Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation

joint with:

Edgar Costa	(Massachusetts Institute of Technology)
Wanlin Li	(Centre de recherches mathématiques)
Bjorn Poonen	(Massachusetts Institute of Technology)
Alexander Smith	(Massachusetts Institute of Technology)

Massachusetts Institute of Technology

Abelian varieties over finite fields

Let $q = p^e$ be a prime power, which will be fixed throughout most of this talk.

Definition

An *abelian variety* of dimension g over $\mathbb{F}_q$ is a smooth irreducible proper variety A of dimension g over $\mathbb{F}_q$ that carries a group structure. The number of points in $A(\mathbb{F}_q)$ is also called the *order* of A.

Example

- Abelian varieties of dimension 1 are elliptic curves.
- The product of two abelian varieties of dimension g_1 and g_2 is an abelian variety of dimension $g_1 + g_2$.
- For a smooth projective irreducible curve C of genus g over $\mathbb{F}_q$, the Jacobian $\mathrm{Jac}(C)$ has the structure of an abelian variety of dimension g.

Isogenies and the order

Definition

An *isogeny* $f : A_1 \to A_2$ from one abelian variety to another, is a morphism that respects both the structure as a variety and the group structure, such that f is surjective on $\overline{\mathbb{F}}_q$-points and $\ker(f)$ is 0-dimensional (i.e. finite). The abelian varieties A_1 and A_2 are then called *isogenous*.

The kernel of an isogeny is a finite subgroup of A_1. On the other hand, if we are given such a finite subgroup $K \subset A_1$, an isogeny $A_1 \to A_1/K$ can be constructed, and A_1/K will have the structure of an abelian variety.

It is not hard to see that isogenous abelian varieties have the same dimension. The following, however, might be more surprising.

Lemma

Let A_1 and A_2 be isogenous abelian varieties over $\mathbb{F}_q$, then A_1 and A_2 have the same order.

Torsion and the Tate module

Let A be an abelian variety over $\mathbb{F}_q$. If ℓ is a prime number, then

$$A(\overline{\mathbb{F}}_q)[\ell] \cong \begin{cases} (\mathbb{Z}/\ell\mathbb{Z})^{2g} & \text{if } \ell \neq p; \\ (\mathbb{Z}/p\mathbb{Z})^{r} & \text{if } \ell = p, \end{cases}$$

for some integer $r \in \{0, \ldots, g\}$, which is called the *p-rank* of A.

Definition

The *Tate module* $T_\ell(A)$ is defined as

$$T_\ell(A) := \lim_{n \in \mathbb{Z}_{>0}} A(\overline{\mathbb{F}}_q)[\ell^n],$$

where the transition maps are given by multiplication-by-ℓ. This has the natural structure of a $\mathbb{Z}_\ell$-module, and we define $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

For $\ell \neq p$, we see that $V_\ell(A)$ is non-canonically isomorphic to $\mathbb{Q}_\ell^{2g}$, and that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on this vector space. In particular, Frob_q acts on this vector space.

Weil polynomials and Honda-Tate theory

Theorem

The characteristic polynomial $f_A(x)$ of Frob_q acting on $V_\ell(A)$ does not depend on the choice of $\ell \neq p$ and has the following properties:

α) *f_A has coefficients in $\mathbb{Z}$, and is monic of degree $2g$;*

β) *f_A is q-symmetric, meaning that it is of the shape*

$$x^{2g} + a_1 x^{2g-1} + \cdots + a_{g-1} x^{g-1} + a_g x^g + q a_{g-1} x^{g+1} + \cdots + q^{g-1} a_1 x + q^g;$$

γ) *all complex roots of f_A have absolute value $q^{1/2}$.*

There is a correspondence between isogeny classes of abelian varieties and *Weil polynomials* (polynomials that occur as f_A). Below we state this in the case of ordinary abelian varieties, i.e. abelian varieties whose p-rank is g.

Theorem (Honda-Tate theory)

There is a correspondence between isogeny classes of ordinary abelian varieties over $\mathbb{F}_q$ and polynomials $f \in \mathbb{Z}[x]$ satisfying conditions α, β, and γ, and the additional condition that the middle coefficient of f is not $0 \bmod p$.

Hasse-Weil inequalities

The order of A turns out to equal $f_A(1)$. As a consequence of the properties of f_A, one can deduce the following.

Theorem (Hasse-Weil)

Let n be the order of an abelian variety of dimension g over $\mathbb{F}_q$. Then

$$(q - 2q^{1/2} + 1)^g \leq n \leq (q + 2q^{1/2} + 1)^g.$$

The main consequence of our work is the following theorem, which says that these Hasse-Weil bounds are optimal "up to a constant".

Theorem (vBCLPS)

For g sufficiently large, every integer in the interval

$$\left[(q - 2q^{1/2} + 3 - q^{-1})^g, (q + 2q^{1/2} - 1 - q^{-1})^g\right]$$

occurs at the order of some geometrically simple ordinary principally polarised abelian variety of dimension g over $\mathbb{F}_q$.

Comparison with previous work of Aubry-Haloui-Lachaud and Kadets

In previous works of Aubry-Haloui-Lachaud and Kadets, the interval

$$I_{\text{simple}} = \left[\liminf_{A \text{ simple}} |A(\mathbb{F}_q)|^{1/\dim A}, \limsup_{A \text{ simple}} |A(\mathbb{F}_q)|^{1/\dim A}\right]$$

has been studied. They gave inner and outer bounds for this interval.

$$\left[q - \lfloor 2q^{1/2} \rfloor + 3, q + \lfloor 2q^{1/2} \rfloor - 1 - q^{-1}\right] \subset I_{\text{simple}} \subset \left[q - \lceil 2q^{1/2} \rceil + 2, q + 2\lceil 2q^{1/2} \rceil\right]$$

The outer bounds are an improvement compared to the Hasse-Weil bounds. This can be explained by the fact that the abelian varieties with very high or low point counts, are products of low dimensional abelian varieties with high/low point counts. Hence, these are not simple abelian varieties.

Our result can be viewed as an improvement for the inner bounds for the interval I_{simple} in the case q is not a square.

Note that in the previous work, it has not been attempted to construct every order in this interval. Only sequences converging to the extremal points of the inner bounds have been constructed.

Effective versions of our results

As n gets large, the intervals of point counts that we can construct start to overlap. So for any q, all but finitely many positive integers will occur as the order of an abelian variety over $\mathbb{F}_q$. We also have an effective version of this result. This extends previous work of Howe and Kedlaya, who proved that every integer can occur as the order of an ordinary abelian variety over $\mathbb{F}_2$.

Theorem (vBCLPS)

Every integer $\geq q^{3\sqrt{q}\log q}$ occurs as the order of some abelian variety over $\mathbb{F}_q$.
For $q \leq 5$, every integer occurs as the order of an abelian variety over $\mathbb{F}_q$.
For $q = 7$, the only integers that do not occur are 2, 14, and 17.

Remark

If we require the abelian variety to be ordinary, then the order 3 has to be excluded for $q = 4$, and the orders 8 and 73 for have to be excluded in the case $q = 7$.

If we moreover require f_A to be squarefree, then the order 17 has to be excluded for $q = 7$.

Constructing Weil polynomials

As we saw, constructing abelian varieties is equivalent to finding Weil polynomials. To construct potential such Weil polynomials, we take a polynomial $h \in \mathbb{R}[z]$ of degree less than $2g$, and we let

$$\widehat{h}(x) := x^{2g} h(1/x) + q^g h(x/q) \in \mathbb{R}[x] \qquad (\text{e.g. } \widehat{z^i} = x^{2g-i} + q^{g-i} x^i).$$

This polynomial $\widehat{h}$ is q-symmetric by construction. Getting the coefficients of $\widehat{h}$ to lie in $\mathbb{Z}$ requires putting conditions of the form

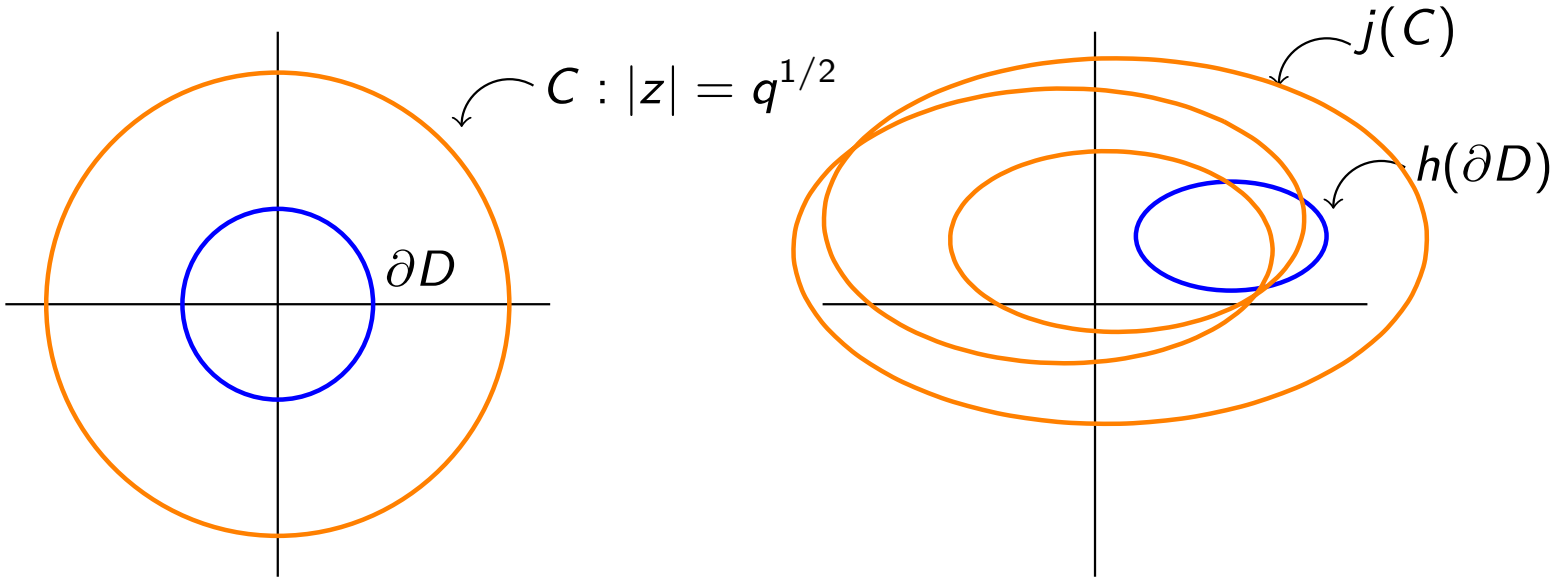
$$h^{[i]} + q^{i-g} h^{[2g-i]} \in \mathbb{Z}, \quad \text{for } i = 0, \ldots, g$$

where $h^{[i]}$ is the coefficient of z^i in h. To get the roots of $\widehat{h}$ to have absolute value $q^{1/2}$, we use the following key lemma.

Key lemma

Let $D = \{|z| \leq q^{-1/2}\} \subset \mathbb{C}$. Suppose that h has no zeros inside the disk D. Then all roots of $\widehat{h}$ have absolute value $q^{1/2}$.

Proof of key lemma



Picture due to Wanlin Li

Proof.

The winding number of $h(\partial D)$ around 0 is 0. Therefore, the winding number of $j(x) = x^g h(1/x)$ around 0 as x traverses C equals g. In particular, the function $\mathrm{Re}(j(x)) = \frac{1}{2}\widehat{h}(x)$ has $2g$ roots on the circle C. □

Overview of the simple method

Goal

Construct a polynomial $h(z) \in \mathbb{R}[z]$ such that

- h has degree at most $2g-1$ and constant coefficient 1;
- $h^{[i]} + q^{i-g} h^{[2g-i]} \in \mathbb{Z}$ and $2h^{[g]} \not\equiv 0 \bmod p$;
- h has no zeros on D;
- $\widehat{h}(1) = h(1) + q^g h(1/q) = n$ (desired order of abelian variety).

Simple method

1. *Start with a power series $j \in \mathbb{Z}[\![z]\!]$ such that j has no zeros on D and*
$$q^g j(1/q) = n.$$
2. *Truncate j into a polynomial h of degree g.*
3. *Add a multiple of z^g to h to correct the value of $\widehat{h}(1)$.*
4. *If needed, make an adjustment to h to assure $\widehat{h}^{[g]} \not\equiv 0 \bmod p$.*
5. *Verify that h has no zeros on D.*

Example of the simple method

Example ($q = 3$ and $n = 16007$)

Step 1. Consider power series of the form

$$j_0(z) = 1 + c_2 z^2 + c_3 z^3 + \ldots \in \mathbb{Z}[\![z]\!], \quad \text{with } c_i \in \{-1, 0, 1\}.$$

Then we see that $j(\frac{1}{3})$ can range between all values in $[\frac{5}{6}, \frac{7}{6}]$.

We see that $3^8 < n < 3^9$, and $\frac{n}{3^9} \approx 0.8132$, so n is closer to 3^9, so we pick $g = 9$. Moreover, $\frac{n}{3^9}$ is smaller than $\frac{5}{6}$, but greater than $(\frac{5}{6})^2$.

Therefore, there is some choice of $c_2, c_3, \ldots$, such that

$$j_0(\tfrac{1}{3})^2 = \frac{n}{3^9}, \qquad \text{or} \qquad 3^9 \cdot j_0(\tfrac{1}{3})^2 = n.$$

Now we take $j = j_0^2$ as a starting point. By construction j_0 satisfies

$$|j(z)| \geq 1 - \frac{1}{3(1 - \frac{1}{\sqrt{3}})} \approx 0.2113 \qquad \text{for all } z \in D.$$

Step 2. It turns out that

$$h(z) = 1 - 2z^2 + 3z^4 - 2z^6 + 2z^7 + 3z^8 - 4z^9.$$

Example of the simple method

Example ($q = 3$ and $n = 16007$, continued)

Step 3. We have $\widehat{h}(1) = 16008$, so we add $-\frac{1}{2}z^9$ to get $\widehat{h}(1) = n$.

Step 4. We now have $\widehat{h}^{[9]} = -9 \equiv 0 \bmod 3$, so we add $z^8 - 2z^9$ to h. This does not change the value of $\widehat{h}(1)$, but it does cause $\widehat{h}^{[9]} = -13 \not\equiv 0 \bmod 3$.

Step 5. Let $z \in D$. We will use the triangle inequality to bound $|h(z)|$ from below. We start with

$$|j(z)|^2 \geq \left(1 - \frac{1}{3(1 - \frac{1}{\sqrt{3}})}\right)^2 \approx 0.0447.$$

The truncation to a polynomial causes this value to decrease at most by

$$3^{-10/2} + 3^{-11/2} + \ldots = \frac{1}{3^{10}(1 - \frac{1}{\sqrt{3}})} \approx 0.00004.$$

Also considering the changes in Step 3 and Step 4, we get

$$|h(z)| \geq 0.0447 - 0.00004 - \tfrac{1}{2} \cdot 3^{-9/2} - 3^{-8/2} - 2 \cdot 3^{-9/2} \approx 0.0144,$$

which indeed ensures that h has no zeros on D.

Difference between our different methods

The **simple method** has the following advantages and disadvantages.

- The simple method already shows that every large enough n is the order of an abelian variety over $\mathbb{F}_q$.
- It is easy to explain and you can actually use it in practice to find Weil polynomials.
- It is hard to get the abelian varieties that we construct to be simple with this method.

Our **advanced method** has the following advantages and disadvantages.

- The method kicks in only for very large values of n, making it infeasible to use in practice.
- Asymptotically, it gives much better results.
- It is easy to impose geometric simplicity on the abelian varieties that we construct.

Our third method, the **effective method** is an improved version of the simple method. It gives a practical algorithm and a reasonable upper bound for the maximum integer that cannot occur as the order of an abelian variety.

Sketch of the advanced method

Idea of the advanced method

- *Instead of a polynomial h of degree g with coefficients in $\mathbb{Z}$, we start with a polynomial of degree $\approx 2g - \log g$ with coefficients in $\mathbb{R}$.*
- *The starting polynomial h is chosen such that it is of the shape P^d for some polynomial P of relatively small degree with $P(0) = 1$. Moreover, P is constructed in such a way that it is as large enough on the disk D, while allowing for as many values of $\widehat{h}(1)$ as possible, i.e. allowing for as many orders of abelian varieties as possible.*
- *From the outside to the inside, we make all the coefficients of h integral. We do this by adding polynomials of the shape $z^i P^j$ to h. In each step we make sure that the value $\widehat{h}(1)$ stays equal to n.*
- *Because we are adding powers of P^j to h, we can obtain better lower bounds on D than by just using the triangle inequality as before.*

Remark

Finding a P that is optimal for our problem, reduces to a problem in potential theory. In the appendix of our preprint, this potential theoretic problem is solved and P is found in terms of Chebyshev polynomials.

Weil polynomials and base change

Suppose that the Weil polynomial f_A of A over $\mathbb{F}_q$ has roots $\{\alpha_1, \ldots, \alpha_{2g}\}$. Then the Weil polynomial $f_{A,e}$ of the base change $A_{\mathbb{F}_{q^e}}$ has $\{\alpha_1^e, \ldots, \alpha_{2g}^e\}$ as roots. The roots of $f_{A,e}$ come in pairs $\{\alpha_i, q^e/\alpha_i\}$, so there is a monic polynomial $R_{A,e} \in \mathbb{Z}[x]$ of degree g satisfying $f_{A,e}(x) = x^n R_{A,e}(x + \frac{q^e}{x})$.

Proposition

Suppose $R_{A,1}$ is irreducible and A is not geometrically simple. Then $\alpha_i = \zeta\alpha_j$ for some $i, j \in \{1, \ldots, 2g\}$ such that $\alpha_j \neq \alpha_i \neq \frac{q}{\alpha_j}$, and some root of unity ζ.

Proof.

If A is isogenous to $A_1 \times A_2$ over $\mathbb{F}_{q^e}$ then $R_{A,e} = R_{A_1,e} \cdot R_{A_2,e}$. The absolute Galois group of $\mathbb{Q}$ acts transitively on the roots of $R_{A,1}$, so the only way in which $R_{A,e}$ is not irreducible, is if some of its roots collapse.

This means that

$$\alpha_i^e + \frac{q^e}{\alpha_i^e} = \alpha_j^e + \frac{q^e}{\alpha_j^e}$$

for some α_i and α_j coming from different pairs. In particular, we get that either $\alpha_i = \zeta\alpha_j$ or $\alpha_i = \zeta\frac{q}{\alpha_j}$, for some e-th root of unity ζ. □

A sufficient condition for geometric simplicity

Lemma

Suppose $g \geq 5$ and $R_{A,1}$ has Galois group S_g, then A is geometrically simple.

Proof.

Suppose A is not geometrically simple, and let α_i and α_j be as in the proposition. Then the extension

$$\mathbb{Q}(\alpha_i + \tfrac{q}{\alpha_i}) \subset \mathbb{Q}(\alpha_i, \zeta) = \mathbb{Q}(\alpha_i, \alpha_j)$$

is a compositum of abelian extensions, hence it is abelian. Therefore, the subextension

$$\mathbb{Q}(\alpha_i + \tfrac{q}{\alpha_i}) \subset \mathbb{Q}(\alpha_i + \tfrac{q}{\alpha_i}, \alpha_j + \tfrac{q}{\alpha_j})$$

is Galois. This is in contradiction with the fact that S_{g-2} is not a normal subgroup of S_{g-1}. □

Goal

Construct h in such a way that $R_{A,1}$ has Galois group S_g.

Congruence conditions

Idea

By imposing a congruence condition

$$\widehat{h}(x) \equiv h_\ell(x) \bmod \ell$$

for some polynomial $h_\ell(x) \in \mathbb{F}_\ell[x]$, we can get the Galois group of $R_{A,1}$ to contain certain cycle types. If we have enough different cycle types, then the Galois group is guaranteed to be S_g.

We can adjust our advanced method to construct polynomials satisfying these congruence conditions, but there are some caveats:

- The set of primes ℓ that we can use have to be fixed in advance, and are not allowed to depend on the order n we want to construct.
- Due to the condition $\widehat{h}(1) = n$ that we require, it could happen that $h_\ell(1) \equiv 0 \bmod \ell$ for all ℓ. In this case, we cannot get the Galois group to be S_g. We can get S_{g-1} and have to do a little bit of extra work.
- The degree of the polynomial $\widehat{h}(x)$ can be arbitrarily large, but ℓ is fixed. So we cannot impose conditions like $h_\ell(x)$ being completely split, as there might not be enough element in $\mathbb{F}_\ell$ to realise that.

More conditions

Congruence conditions can also be put to get the following properties:

- the isogeny class of A contains a principally polarisable abelian variety, using a result of Howe;
- A has p-rank $r(g)$, where $r(g)$ is a function $\mathbb{Z}_{\geq 0} \to \mathbb{Z}$ such that $r(g) \in \{0, \ldots, g\}$ (e.g. to get A is ordinary, we take $r(g) = g$).

Instead of asking for the order of $A(\mathbb{F}_q)$ to be prescribed, we could ask for a specific group structure for $A(\mathbb{F}_q)$. By looking at the action of the endomorphism algebra, Marseglia and Springer showed the following.

Proposition (Marseglia-Springer)

Every square-free ordinary isogeny class over $\mathbb{F}_q$ contains an abelian variety such that $A(\mathbb{F}_q)$ is a cyclic group.

In particular, our method can be used to produce abelian varieties having cyclic groups. This does not mean that every large enough group will occur as $A(\mathbb{F}_q)$. For example, when $q > 10$, the group $(\mathbb{Z}/2\mathbb{Z})^{2g}$ for g very large cannot occur, as the structure of the group requires the dimension of A to be at least g, but the size of the group will contradict the Hasse-Weil bounds.

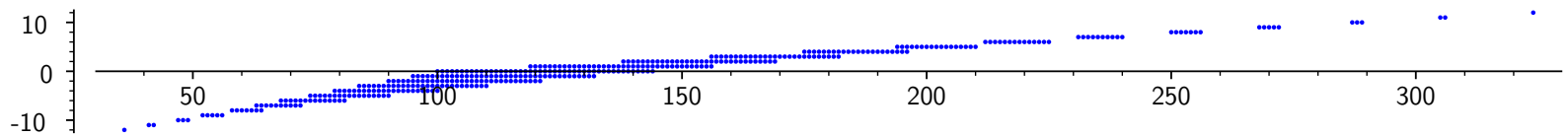
Idea for the large q limit

Again write $f_A(x) = x^g R(x + \frac{q}{x})$ for some monic polynomial $R(x) \in \mathbb{Z}[x]$. If

$$R(x) = x^g + c_1 x^{g-1} + \ldots + c_n,$$

then the Hasse-Weil inequalities give us that $c_i = \mathcal{O}(q^{i/2})$. On the other hand, the order of A is

$$f_A(1) = (q+1)^g + c_1(q+1)^{g-1} + \ldots + c_n.$$



Idea

If we fix c_1, we get an interval I_{c_1} containing all potential orders that we can obtain by varying $c_2, \ldots, c_n$ along their allowed ranges. We have:

- if c_1 is not too close to the extreme values, every order in the interval I_{c_1} can be realised;
- if c_1 is close to one of the extreme values, then the intervals I_{c_1} and I_{c_1+1} do not overlap, proving that some orders cannot be realised.

Statement

Theorem (vBCLPS)

Let $g \geq 3$ and $\lambda := 2g - \sqrt{\frac{2g}{g-1}}$. Then the largest interval in which every integer is the order of some g-dimensional abelian variety over $\mathbb{F}_q$ is of the shape

$$\left[q^g - \lambda q^{g-\frac{1}{2}} + o(q^{g-\frac{1}{2}}), \quad q^g + \lambda q^{g-\frac{1}{2}} + o(q^{g-\frac{1}{2}})\right],$$

as $q \to \infty$ through prime powers.

Remark

For the case of elliptic curves over prime fields, every order in the Hasse-Weil interval can be realised. That means that the theorem is still true if you take $\lambda = 2$ and q prime. For prime powers, there will be some orders in the Hasse-Weil interval that cannot be realised. This is caused by polynomials whose middle coefficient is 0 mod p and are not Weil polynomials.

For the case $g = 2$, the statement is still true if we either require q to be prime, or if we take $\lambda = 4 - 2\sqrt{2}$ instead of $\lambda = 2$. This is again caused by polynomials whose middle coefficient is 0 mod p.

Summary

We discussed:

- how to use Honda-Tate theory to construct abelian varieties over $\mathbb{F}_q$;
- three methods to construct Weil polynomials: simple, advanced, and effective method;
- how to use congruence conditions to impose geometric simplicity, and other properties;
- some results in the large q-limit.