Weil polynomials for fun and profit

Kiran S. Kedlaya

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

Number Theory Informed by Computation
Park City Mathematics Institute, Park City, Utah
July 26, 2022

Supported by NSF (grants DMS-2053473 and prior) and UC San Diego (Warschawski Professorship).

The UC San Diego campus sits on unceded ancestral land of the Kumeyaay Nation. The Kumeyaay people continue to have an important and thriving presence in the region.

Contents

What is a Weil polynomial?

Fix a prime power q. A q-**Weil polynomial** is* a monic polynomial $P(T) \in \mathbb{Z}[T]$ whose roots in $\mathbb{C}$ all lie on the circle $|T| = \sqrt{q}$.

For example, $T^2 + aT + q$ is a q-Weil polynomial if and only if $|a| \leq 2\sqrt{q}$.

Exercise: for fixed g and q, there are finitely many q-Weil polynomials of degree $2g$. You can compute this set easily in Sage! (Demo to follow.)

```
sage: P.<x> = QQ[]
sage: l = P.weil_polynomials(6, 2)
sage: len(l)
215
sage: l[0]
x^6 + 6*x^5 + 18*x^4 + 32*x^3 + 36*x^2 + 24*x + 8
```

*For the purposes of this talk anyway. Conventions may vary between sources.

What is a Weil polynomial?

Fix a prime power q. A q-**Weil polynomial** is* a monic polynomial $P(T) \in \mathbb{Z}[T]$ whose roots in $\mathbb{C}$ all lie on the circle $|T| = \sqrt{q}$.

For example, $T^2 + aT + q$ is a q-Weil polynomial if and only if $|a| \leq 2\sqrt{q}$.

Exercise: for fixed g and q, there are finitely many q-Weil polynomials of degree $2g$. You can compute this set easily in Sage! (Demo to follow.)

```
sage: P.<x> = QQ[]
sage: l = P.weil_polynomials(6, 2)
sage: len(l)
215
sage: l[0]
x^6 + 6*x^5 + 18*x^4 + 32*x^3 + 36*x^2 + 24*x + 8
```

*For the purposes of this talk anyway. Conventions may vary between sources.

What is a Weil polynomial?

Fix a prime power q. A q-**Weil polynomial** is* a monic polynomial $P(T) \in \mathbb{Z}[T]$ whose roots in $\mathbb{C}$ all lie on the circle $|T| = \sqrt{q}$.

For example, $T^2 + aT + q$ is a q-Weil polynomial if and only if $|a| \leq 2\sqrt{q}$.

Exercise: for fixed g and q, there are finitely many q-Weil polynomials of degree $2g$. You can compute this set easily in Sage! (Demo to follow.)

```
sage: P.<x> = QQ[]
sage: l = P.weil_polynomials(6, 2)
sage: len(l)
215
sage: l[0]
x^6 + 6*x^5 + 18*x^4 + 32*x^3 + 36*x^2 + 24*x + 8
```

*For the purposes of this talk anyway. Conventions may vary between sources.

How do Weil polynomials arise in number theory?

For X an algebraic variety over $\mathbb{F}_q$, the **zeta function** of X is the power series

$$Z(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \#X(\mathbb{F}_{q^n})\right) \in \mathbb{Z}[\![T]\!].$$

(Exercise: why $\mathbb{Z}$ and not $\mathbb{Q}$?) If X is smooth proper of dimension d, then

$$Z(X, T) = \frac{L_1(T) \cdots L_{2d-1}(T)}{L_0(T)L_2(T) \cdots L_{2d}(T)}$$

where $L_i(T)$ is the **reverse** of a q^i-Weil polynomial.†

This statement is a consequence of the **Weil conjectures** (which are now theorems). Weil was led to these conjectures by computing some classical examples like **Gauss sums** and **Jacobi sums**.

†The reverses of Weil polynomials are sometimes called L-**polynomials**.

How do Weil polynomials arise in number theory?

For X an algebraic variety over $\mathbb{F}_q$, the **zeta function** of X is the power series

$$Z(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \# X(\mathbb{F}_{q^n})\right) \in \mathbb{Z}[\![T]\!].$$

(Exercise: why $\mathbb{Z}$ and not $\mathbb{Q}$?) If X is smooth proper of dimension d, then

$$Z(X, T) = \frac{L_1(T) \cdots L_{2d-1}(T)}{L_0(T) L_2(T) \cdots L_{2d}(T)}$$

where $L_i(T)$ is the **reverse** of a q^i-Weil polynomial.†

This statement is a consequence of the **Weil conjectures** (which are now theorems). Weil was led to these conjectures by computing some classical examples like **Gauss sums** and **Jacobi sums**.

†The reverses of Weil polynomials are sometimes called L-**polynomials**.

Examples

For $X = \mathbb{P}^n$,

$$Z(X, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}.$$

For X a curve of genus g,

$$Z(X, T) = \frac{P_1(T)}{(1-T)(1-qT)}.$$

For X an abelian variety of dimension d,

$$P_i(T) = \wedge^i P_1(T) \qquad (i = 0, \dots, 2d).$$

That is, the roots of $P_i(T)$ are the i-fold products of roots of $P_1(T)$.

Important point: a curve and its Jacobian have the same $P_1(T)$.

Examples

For $X = \mathbb{P}^n$,

$$Z(X, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^n T)}.$$

For X a curve of genus g,

$$Z(X, T) = \frac{P_1(T)}{(1-T)(1-qT)}.$$

For X an abelian variety of dimension d,

$$P_i(T) = \wedge^i P_1(T) \qquad (i = 0, \dots, 2d).$$

That is, the roots of $P_i(T)$ are the i-fold products of roots of $P_1(T)$.

Important point: a curve and its Jacobian have the same $P_1(T)$.

Examples

For $X = \mathbb{P}^n$,

$$Z(X, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}.$$

For X a curve of genus g,

$$Z(X, T) = \frac{P_1(T)}{(1-T)(1-qT)}.$$

For X an abelian variety of dimension d,

$$P_i(T) = \wedge^i P_1(T) \qquad (i = 0, \dots, 2d).$$

That is, the roots of $P_i(T)$ are the i-fold products of roots of $P_1(T)$.

Important point: a curve and its Jacobian have the same $P_1(T)$.

Examples

For $X = \mathbb{P}^n$,

$$Z(X, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}.$$

For X a curve of genus g,

$$Z(X, T) = \frac{P_1(T)}{(1-T)(1-qT)}.$$

For X an abelian variety of dimension d,

$$P_i(T) = \wedge^i P_1(T) \qquad (i = 0, \dots, 2d).$$

That is, the roots of $P_i(T)$ are the i-fold products of roots of $P_1(T)$.

Important point: a curve and its Jacobian have the same $P_1(T)$.

Weil polynomials and abelian varieties

Hereafter take $X = A$ to be an abelian variety over $\mathbb{F}_q$ and let $P_A(T)$ be the reverse of $L_1(T)$. This is the charpoly of Frobenius acting on the ℓ-adic Tate module of A for any prime ℓ not dividing q.

The Honda–Tate theorem has the following consequences:

- $P_A(T)$ is a complete invariant for **isogeny classes** of abelian varieties;
- "almost" every q-Weil polynomial occurs as $P_A(T)$ for some A. More precisely, every q-Weil polynomial has a power that occurs, and the minimal such power is easily computable.

This can be used to tabulate isogeny classes of abelian varieties. This was done in LMFDB by Dupuy–K–Roe–Vincent. (Demo to follow.)

Weil polynomials and abelian varieties

Hereafter take $X = A$ to be an abelian variety over $\mathbb{F}_q$ and let $P_A(T)$ be the reverse of $L_1(T)$. This is the charpoly of Frobenius acting on the ℓ-adic Tate module of A for any prime ℓ not dividing q.

The Honda–Tate theorem has the following consequences:

- $P_A(T)$ is a complete invariant for **isogeny classes** of abelian varieties;
- "almost" every q-Weil polynomial occurs as $P_A(T)$ for some A. More precisely, every q-Weil polynomial has a power that occurs, and the minimal such power is easily computable.

This can be used to tabulate isogeny classes of abelian varieties. This was done in LMFDB by Dupuy–K–Roe–Vincent. (Demo to follow.)

Weil polynomials and abelian varieties

Hereafter take $X = A$ to be an abelian variety over $\mathbb{F}_q$ and let $P_A(T)$ be the reverse of $L_1(T)$. This is the charpoly of Frobenius acting on the ℓ-adic Tate module of A for any prime ℓ not dividing q.

The Honda–Tate theorem has the following consequences:

- $P_A(T)$ is a complete invariant for **isogeny classes** of abelian varieties;
- "almost" every q-Weil polynomial occurs as $P_A(T)$ for some A. More precisely, every q-Weil polynomial has a power that occurs, and the minimal such power is easily computable.

This can be used to tabulate isogeny classes of abelian varieties. This was done in LMFDB by Dupuy–K–Roe–Vincent. (Demo to follow.)

Weil polynomials and abelian varieties

Hereafter take $X = A$ to be an abelian variety over $\mathbb{F}_q$ and let $P_A(T)$ be the reverse of $L_1(T)$. This is the charpoly of Frobenius acting on the ℓ-adic Tate module of A for any prime ℓ not dividing q.

The Honda–Tate theorem has the following consequences:

- $P_A(T)$ is a complete invariant for **isogeny classes** of abelian varieties;
- "almost" every q-Weil polynomial occurs as $P_A(T)$ for some A. More precisely, every q-Weil polynomial has a power that occurs, and the minimal such power is easily computable.

This can be used to tabulate isogeny classes of abelian varieties. This was done in LMFDB by Dupuy–K–Roe–Vincent. (Demo to follow.)

Weil polynomials and abelian varieties

Hereafter take $X = A$ to be an abelian variety over $\mathbb{F}_q$ and let $P_A(T)$ be the reverse of $L_1(T)$. This is the charpoly of Frobenius acting on the ℓ-adic Tate module of A for any prime ℓ not dividing q.

The Honda–Tate theorem has the following consequences:

- $P_A(T)$ is a complete invariant for **isogeny classes** of abelian varieties;
- "almost" every q-Weil polynomial occurs as $P_A(T)$ for some A. More precisely, every q-Weil polynomial has a power that occurs, and the minimal such power is easily computable.

This can be used to tabulate isogeny classes of abelian varieties. This was done in LMFDB by Dupuy–K–Roe–Vincent. (Demo to follow.)

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

What can Weil polynomials tell us?

From $P_A(T)$, the following information about A is readily available:

- The group orders $\#A(\mathbb{F}_{q^n})$.
- The p-**rank** and **Newton polygon** of A.
- The **angle rank** of A (to be defined later).
- If A is the Jacobian of a curve C, the counts $\#C(\mathbb{F}_{q^n})$.

The following information is **not uniquely determined** in general:

- The isomorphism classes of the groups $\#A(\mathbb{F}_{q^n})$.
- The p-**divisible group**, **formal group**, and a-**number** of A.

The following information is available **in principle**:

- The isomorphism classes of abelian varieties isogenies to A.
- The polarization degrees of said abelian varieties.
- The isomorphism classes of curves C with Jacobian isogenous to A.

Contents

Abelian varieties of prescribed order

For A an abelian variety over $\mathbb{F}_q$, we have

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

Using this, one can show that:

- for $q = 2$, every positive integer occurs as $\#A(\mathbb{F}_q)$ (Howe–K);
- for fixed $q > 2$, every sufficiently large integer occurs (van Bommel–Costa–Li–Poonen–Smith);
- for $q = 2$, every positive integer occurs infinitely often with A simple (K);
- for $q = 2$, the simple abelian varieties of order 1 can be completely classified (Madan–Pal), along with their $\overline{\mathbb{F}}_2$-simple factors (K–D'Nelly-Warady).

Abelian varieties of prescribed order

For A an abelian variety over $\mathbb{F}_q$, we have

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

Using this, one can show that:

- for $q = 2$, every positive integer occurs as $\#A(\mathbb{F}_q)$ (Howe–K);
- for fixed $q > 2$, every sufficiently large integer occurs (van Bommel–Costa–Li–Poonen–Smith);
- for $q = 2$, every positive integer occurs infinitely often with A simple (K);
- for $q = 2$, the simple abelian varieties of order 1 can be completely classified (Madan–Pal), along with their $\overline{\mathbb{F}}_2$-simple factors (K–D'Nelly-Warady).

Abelian varieties of prescribed order

For A an abelian variety over $\mathbb{F}_q$, we have

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

Using this, one can show that:

- for $q = 2$, every positive integer occurs as $\#A(\mathbb{F}_q)$ (Howe–K);
- for fixed $q > 2$, every sufficiently large integer occurs (van Bommel–Costa–Li–Poonen–Smith);
- for $q = 2$, every positive integer occurs infinitely often with A simple (K);
- for $q = 2$, the simple abelian varieties of order 1 can be completely classified (Madan–Pal), along with their $\overline{\mathbb{F}}_2$-simple factors (K–D'Nelly-Warady).

Abelian varieties of prescribed order

For A an abelian variety over $\mathbb{F}_q$, we have

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

Using this, one can show that:

- for $q = 2$, every positive integer occurs as $\#A(\mathbb{F}_q)$ (Howe–K);
- for fixed $q > 2$, every sufficiently large integer occurs (van Bommel–Costa–Li–Poonen–Smith);
- for $q = 2$, every positive integer occurs infinitely often with A simple (K);
- for $q = 2$, the simple abelian varieties of order 1 can be completely classified (Madan–Pal), along with their $\overline{\mathbb{F}}_2$-simple factors (K–D'Nelly-Warady).

Abelian varieties of prescribed order

For A an abelian variety over $\mathbb{F}_q$, we have

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

Using this, one can show that:

- for $q = 2$, every positive integer occurs as $\#A(\mathbb{F}_q)$ (Howe–K);
- for fixed $q > 2$, every sufficiently large integer occurs (van Bommel–Costa–Li–Poonen–Smith);
- for $q = 2$, every positive integer occurs infinitely often with A simple (K);
- for $q = 2$, the simple abelian varieties of order 1 can be completely classified (Madan–Pal), along with their $\overline{\mathbb{F}}_2$-simple factors (K–D'Nelly-Warady).

The number of rational points on a curve

For given g, q, what is the maximum of $\#C(\mathbb{F}_q)$ over all genus-g curves over $\mathbb{F}_q$? The answer has implications in coding theory (Goppa).

One can improve on the Weil bound via linear programming on Weil's explicit formula (Ihara, Drinfeld–Vlăduț, Oesterlé, Serre).

One can often do **slightly** better by classifying the Weil polynomials compatible with a putative point count, then ruling them out one by one (Serre, Lauter, Howe–Lauter, etc.).

For known upper and lower bounds in many cases, see manypoints.org.

The number of rational points on a curve

For given g, q, what is the maximum of $\#C(\mathbb{F}_q)$ over all genus-g curves over $\mathbb{F}_q$? The answer has implications in coding theory (Goppa).

One can improve on the Weil bound via linear programming on Weil's explicit formula (Ihara, Drinfeld–Vlăduț, Oesterlé, Serre).

One can often do **slightly** better by classifying the Weil polynomials compatible with a putative point count, then ruling them out one by one (Serre, Lauter, Howe–Lauter, etc.).

For known upper and lower bounds in many cases, see manypoints.org.

The number of rational points on a curve

For given g, q, what is the maximum of $\#C(\mathbb{F}_q)$ over all genus-g curves over $\mathbb{F}_q$? The answer has implications in coding theory (Goppa).

One can improve on the Weil bound via linear programming on Weil's explicit formula (Ihara, Drinfeld–Vlăduț, Oesterlé, Serre).

One can often do **slightly** better by classifying the Weil polynomials compatible with a putative point count, then ruling them out one by one (Serre, Lauter, Howe–Lauter, etc.).

For known upper and lower bounds in many cases, see manypoints.org.

The number of rational points on a curve

For given g, q, what is the maximum of $\#C(\mathbb{F}_q)$ over all genus-g curves over $\mathbb{F}_q$? The answer has implications in coding theory (Goppa).

One can improve on the Weil bound via linear programming on Weil's explicit formula (Ihara, Drinfeld–Vlăduț, Oesterlé, Serre).

One can often do **slightly** better by classifying the Weil polynomials compatible with a putative point count, then ruling them out one by one (Serre, Lauter, Howe–Lauter, etc.).

For known upper and lower bounds in many cases, see manypoints.org.

The relative class number one problem for curves

Let $C' \to C$ be a finite morphism of curves. Then $J(C')$ is isogenous to the product of $J(C)$ with an abelian variety A (the **Prym variety**). The **relative class number** of this covering is $\#A(\mathbb{F}_q)$. When can this equal 1?

For $q > 4$ it is impossible to have $\#A(\mathbb{F}_q) = 1$ unless $A = 0$. For $q = 2, 3, 4$, we know the possible simple factors[‡] of A; this forces C to have "many" points compared to upper bounds as on the previous slide.

This reduces the problem to a still nontrivial finite computation:

- Identify candidate Weil polynomials for C, C' using targeted searches.
- Find all C with the right Weil polynomial (genus up to 7).
- Find all cyclic covers $C' \to C$ of the appropriate degree (up to 7).
- Show that no noncyclic covers can occur.

For more details, watch my ANTS talk in two weeks!

[‡]For $q = 3, 4$, the only possible simple factor is of genus 1.

The relative class number one problem for curves

Let $C' \to C$ be a finite morphism of curves. Then $J(C')$ is isogenous to the product of $J(C)$ with an abelian variety A (the **Prym variety**). The **relative class number** of this covering is $\#A(\mathbb{F}_q)$. When can this equal 1?

For $q > 4$ it is impossible to have $\#A(\mathbb{F}_q) = 1$ unless $A = 0$. For $q = 2, 3, 4$, we know the possible simple factors[‡] of A; this forces C to have "many" points compared to upper bounds as on the previous slide.

This reduces the problem to a still nontrivial finite computation:

- Identify candidate Weil polynomials for C, C' using targeted searches.
- Find all C with the right Weil polynomial (genus up to 7).
- Find all cyclic covers $C' \to C$ of the appropriate degree (up to 7).
- Show that no noncyclic covers can occur.

For more details, watch my ANTS talk in two weeks!

[‡]For $q = 3, 4$, the only possible simple factor is of genus 1.

The relative class number one problem for curves

Let $C' \to C$ be a finite morphism of curves. Then $J(C')$ is isogenous to the product of $J(C)$ with an abelian variety A (the **Prym variety**). The **relative class number** of this covering is $\#A(\mathbb{F}_q)$. When can this equal 1?

For $q > 4$ it is impossible to have $\#A(\mathbb{F}_q) = 1$ unless $A = 0$. For $q = 2, 3, 4$, we know the possible simple factors‡ of A; this forces C to have "many" points compared to upper bounds as on the previous slide.

This reduces the problem to a still nontrivial finite computation:

- Identify candidate Weil polynomials for C, C' using targeted searches.
- Find all C with the right Weil polynomial (genus up to 7).
- Find all cyclic covers $C' \to C$ of the appropriate degree (up to 7).
- Show that no noncyclic covers can occur.

For more details, watch my ANTS talk in two weeks!

‡For $q = 3, 4$, the only possible simple factor is of genus 1.

The relative class number one problem for curves

Let $C' \to C$ be a finite morphism of curves. Then $J(C')$ is isogenous to the product of $J(C)$ with an abelian variety A (the **Prym variety**). The **relative class number** of this covering is $\#A(\mathbb{F}_q)$. When can this equal 1?

For $q > 4$ it is impossible to have $\#A(\mathbb{F}_q) = 1$ unless $A = 0$. For $q = 2, 3, 4$, we know the possible simple factors[‡] of A; this forces C to have "many" points compared to upper bounds as on the previous slide.

This reduces the problem to a still nontrivial finite computation:

- Identify candidate Weil polynomials for C, C' using targeted searches.
- Find all C with the right Weil polynomial (genus up to 7).
- Find all cyclic covers $C' \to C$ of the appropriate degree (up to 7).
- Show that no noncyclic covers can occur.

For more details, watch my ANTS talk in two weeks!

[‡]For $q = 3, 4$, the only possible simple factor is of genus 1.

The relative class number one problem for curves

Let $C' \to C$ be a finite morphism of curves. Then $J(C')$ is isogenous to the product of $J(C)$ with an abelian variety A (the **Prym variety**). The **relative class number** of this covering is $\#A(\mathbb{F}_q)$. When can this equal 1?

For $q > 4$ it is impossible to have $\#A(\mathbb{F}_q) = 1$ unless $A = 0$. For $q = 2, 3, 4$, we know the possible simple factors[‡] of A; this forces C to have "many" points compared to upper bounds as on the previous slide.

This reduces the problem to a still nontrivial finite computation:

- Identify candidate Weil polynomials for C, C' using targeted searches.
- Find all C with the right Weil polynomial (genus up to 7).
- Find all cyclic covers $C' \to C$ of the appropriate degree (up to 7).
- Show that no noncyclic covers can occur.

For more details, watch my ANTS talk in two weeks!

[‡] For $q = 3, 4$, the only possible simple factor is of genus 1.

The relative class number one problem for curves

Let $C' \to C$ be a finite morphism of curves. Then $J(C')$ is isogenous to the product of $J(C)$ with an abelian variety A (the **Prym variety**). The **relative class number** of this covering is $\#A(\mathbb{F}_q)$. When can this equal 1?

For $q > 4$ it is impossible to have $\#A(\mathbb{F}_q) = 1$ unless $A = 0$. For $q = 2, 3, 4$, we know the possible simple factors[‡] of A; this forces C to have "many" points compared to upper bounds as on the previous slide.

This reduces the problem to a still nontrivial finite computation:

- Identify candidate Weil polynomials for C, C' using targeted searches.
- Find all C with the right Weil polynomial (genus up to 7).
- Find all cyclic covers $C' \to C$ of the appropriate degree (up to 7).
- Show that no noncyclic covers can occur.

For more details, watch my ANTS talk in two weeks!

[‡]For $q = 3, 4$, the only possible simple factor is of genus 1.

The relative class number one problem for curves

Let $C' \to C$ be a finite morphism of curves. Then $J(C')$ is isogenous to the product of $J(C)$ with an abelian variety A (the **Prym variety**). The **relative class number** of this covering is $\#A(\mathbb{F}_q)$. When can this equal 1?

For $q > 4$ it is impossible to have $\#A(\mathbb{F}_q) = 1$ unless $A = 0$. For $q = 2, 3, 4$, we know the possible simple factors[‡] of A; this forces C to have "many" points compared to upper bounds as on the previous slide.

This reduces the problem to a still nontrivial finite computation:

- Identify candidate Weil polynomials for C, C' using targeted searches.
- Find all C with the right Weil polynomial (genus up to 7).
- Find all cyclic covers $C' \to C$ of the appropriate degree (up to 7).
- Show that no noncyclic covers can occur.

For more details, watch my ANTS talk in two weeks!

[‡]For $q = 3, 4$, the only possible simple factor is of genus 1.

The relative class number one problem for curves

Let $C' \to C$ be a finite morphism of curves. Then $J(C')$ is isogenous to the product of $J(C)$ with an abelian variety A (the **Prym variety**). The **relative class number** of this covering is $\#A(\mathbb{F}_q)$. When can this equal 1?

For $q > 4$ it is impossible to have $\#A(\mathbb{F}_q) = 1$ unless $A = 0$. For $q = 2, 3, 4$, we know the possible simple factors[‡] of A; this forces C to have "many" points compared to upper bounds as on the previous slide.

This reduces the problem to a still nontrivial finite computation:

- Identify candidate Weil polynomials for C, C' using targeted searches.
- Find all C with the right Weil polynomial (genus up to 7).
- Find all cyclic covers $C' \to C$ of the appropriate degree (up to 7).
- Show that no noncyclic covers can occur.

For more details, watch my ANTS talk in two weeks!

[‡] For $q = 3, 4$, the only possible simple factor is of genus 1.

Angle ranks and the Tate conjecture

The **angle rank** of A is the rank of the subgroup of $\mathbb{C}^\times/q^{\mathbb{Z}}$ generated by the Frobenius eigenvalues; it is in $\{0, \ldots, g\}$. (Exercise: A is supersingular iff its angle rank is 0.)

In generic cases the angle rank equals g. When this occurs, the Tate conjecture holds for A in all degrees.

One can give criteria for full angle rank in terms of Newton polygons; e.g., if g is even and A is **nearly ordinary** then it has full angle rank (Lenstra–Zarhin).

By studying the Galois action on the Frobenius eigenvalues one can give additional such criteria and explain many numerical features of the LMFDB data (Dupuy–K–Zureick-Brown). For details, come celebrate Hendrik Lenstra's birthday in Edinburgh next April!

Angle ranks and the Tate conjecture

The **angle rank** of A is the rank of the subgroup of $\mathbb{C}^\times/q^\mathbb{Z}$ generated by the Frobenius eigenvalues; it is in $\{0, \ldots, g\}$. (Exercise: A is supersingular iff its angle rank is 0.)

In generic cases the angle rank equals g. When this occurs, the Tate conjecture holds for A in all degrees.

One can give criteria for full angle rank in terms of Newton polygons; e.g., if g is even and A is **nearly ordinary** then it has full angle rank (Lenstra–Zarhin).

By studying the Galois action on the Frobenius eigenvalues one can give additional such criteria and explain many numerical features of the LMFDB data (Dupuy–K–Zureick-Brown). For details, come celebrate Hendrik Lenstra's birthday in Edinburgh next April!

Angle ranks and the Tate conjecture

The **angle rank** of A is the rank of the subgroup of $\mathbb{C}^\times/q^\mathbb{Z}$ generated by the Frobenius eigenvalues; it is in $\{0, \dots, g\}$. (Exercise: A is supersingular iff its angle rank is 0.)

In generic cases the angle rank equals g. When this occurs, the Tate conjecture holds for A in all degrees.

One can give criteria for full angle rank in terms of Newton polygons; e.g., if g is even and A is **nearly ordinary** then it has full angle rank (Lenstra–Zarhin).

By studying the Galois action on the Frobenius eigenvalues one can give additional such criteria and explain many numerical features of the LMFDB data (Dupuy–K–Zureick-Brown). For details, come celebrate Hendrik Lenstra's birthday in Edinburgh next April!

Angle ranks and the Tate conjecture

The **angle rank** of A is the rank of the subgroup of $\mathbb{C}^\times/q^{\mathbb{Z}}$ generated by the Frobenius eigenvalues; it is in $\{0,\dots,g\}$. (Exercise: A is supersingular iff its angle rank is 0.)

In generic cases the angle rank equals g. When this occurs, the Tate conjecture holds for A in all degrees.

One can give criteria for full angle rank in terms of Newton polygons; e.g., if g is even and A is **nearly ordinary** then it has full angle rank (Lenstra–Zarhin).

By studying the Galois action on the Frobenius eigenvalues one can give additional such criteria and explain many numerical features of the LMFDB data (Dupuy–K–Zureick-Brown). For details, come celebrate Hendrik Lenstra's birthday in Edinburgh next April!

Contents

Demos

We'll now demonstrate:

- functionality for Weil polynomials in Sage;
- searching through LMFDB for isogeny classes of abelian varieties over finite fields.

Demos

We'll now demonstrate:

- functionality for Weil polynomials in Sage;
- searching through LMFDB for isogeny classes of abelian varieties over finite fields.

Demos

We'll now demonstrate:

- functionality for Weil polynomials in Sage;
- searching through LMFDB for isogeny classes of abelian varieties over finite fields.