Constructing genus 2 curves over finite fields with a prescribed number of points

Chloe Martindale

Technische Universiteit Eindhoven

Joint work with Marco Streng

June 1, 2017

Reminder: Elliptic Curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on E is defined to be

$$\begin{array}{rccc} \pi_q : & E & \longrightarrow & E \\ & P & \mapsto & P^q. \end{array}$$

Reminder: Elliptic Curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on E is defined to be

$$\begin{array}{rccc} \pi_q: & E & \longrightarrow & E \\ & P & \mapsto & P^q. \end{array}$$

- The characteristic polynomial of the Frobenius morphism is of the form
$$\chi_{\pi_q}(X) = X^2 - tX + q.$$

Reminder: Elliptic Curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on E is defined to be

$$\pi_q : \begin{array}{ccc} E & \longrightarrow & E \\ P & \mapsto & P^q. \end{array}$$

- The characteristic polynomial of the Frobenius morphism is of the form
$$\chi_{\pi_q}(X) = X^2 - tX + q.$$
- We call t the *trace of Frobenius*.

Reminder: Elliptic Curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on E is defined to be

$$\begin{array}{rccc} \pi_q : & E & \longrightarrow & E \\ & P & \mapsto & P^q. \end{array}$$

- The characteristic polynomial of the Frobenius morphism is of the form
$$\chi_{\pi_q}(X) = X^2 - tX + q.$$
- We call t the *trace of Frobenius*.
- $\#E(\mathbb{F}_q) = 1 - t + q$

Endomorphisms of elliptic curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. An *endomorphism* of E is a morphism $E \to E$.

Endomorphisms of elliptic curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. An *endomorphism* of E is a morphism $E \to E$.

Examples

- The q-power Frobenius morphism.

Endomorphisms of elliptic curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. An *endomorphism* of E is a morphism $E \to E$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} E & \longrightarrow & E \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

Endomorphisms of elliptic curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. An *endomorphism* of E is a morphism $E \to E$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} E & \longrightarrow & E \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of E form a ring, called the *endomorphism ring* of E, written as $\mathrm{End}(E)$.

Endomorphisms of elliptic curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. An *endomorphism* of E is a morphism $E \to E$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} E & \longrightarrow & E \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of E form a ring, called the *endomorphism ring* of E, written as $\mathrm{End}(E)$.
- To find: $E/\mathbb{F}_q$ such that $\pi \in \mathrm{End}(E)$, where

$$\chi_{\pi_q}(X) = X^2 - tX + q = (X - \pi)(X - \overline{\pi}).$$

Endomorphisms of elliptic curves over finite fields

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. An *endomorphism* of E is a morphism $E \to E$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} E & \longrightarrow & E \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of E form a ring, called the *endomorphism ring* of E, written as $\mathrm{End}(E)$.
- To find: $E/\mathbb{F}_q$ such that $\pi \in \mathrm{End}(E)$, where

$$\chi_{\pi_q}(X) = X^2 - tX + q = (X - \pi)(X - \overline{\pi}).$$

- All such E will satisfy $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$.

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$.

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$
2. $\pi \in \mathrm{End}(E)$

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$
2. $\pi \in \mathrm{End}(E)$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$
2. $\pi \in \mathrm{End}(E)$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$.

Constructing elliptic curves with a given number of points

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Constructing elliptic curves with a given number of points

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Definition

The *class polynomial* for K is defined to be

$$H_K(X) = \prod_{E/\mathbb{C}:\mathrm{End}(E)=\mathcal{O}_K} (X - j(E)) \in \mathbb{Z}[X].$$

Constructing elliptic curves with a given number of points

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Definition

The *class polynomial* for K is defined to be

$$H_K(X) = \prod_{E/\mathbb{C}:\mathrm{End}(E)=\mathcal{O}_K} (X - j(E)) \in \mathbb{Z}[X].$$

- This polynomial has integral coefficients!

Constructing elliptic curves with a given number of points

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Definition

The *class polynomial* for K is defined to be

$$H_K(X) = \prod_{E/\mathbb{C}:\mathrm{End}(E)=\mathcal{O}_K} (X - j(E)) \in \mathbb{Z}[X].$$

- This polynomial has integral coefficients!
- The roots of $H_K(X)$ mod q are the j-invariants of all the elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Constructing elliptic curves with a given number of points

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Definition

The *class polynomial* for K is defined to be

$$H_K(X) = \prod_{E/\mathbb{C}:\mathrm{End}(E)=\mathcal{O}_K} (X - j(E)) \in \mathbb{Z}[X].$$

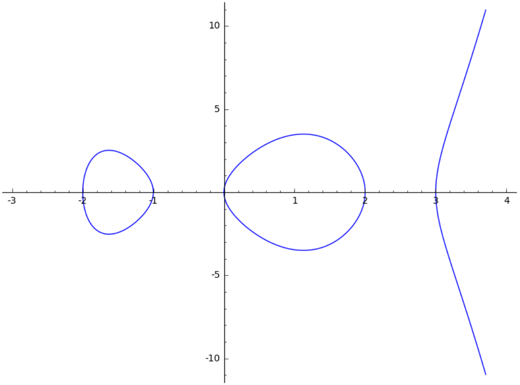
- This polynomial has integral coefficients!
- The roots of $H_K(X)$ mod q are the j-invariants of all the elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
- There is an algorithm to enumerate all the elliptic curves with $1 - t + q$ points given those with endomorphism ring $\mathcal{O}_K$.

Genus 2 curves

- A genus 2 curve C over a finite field $\mathbb{F}_q$, with q odd, has a hyperelliptic model

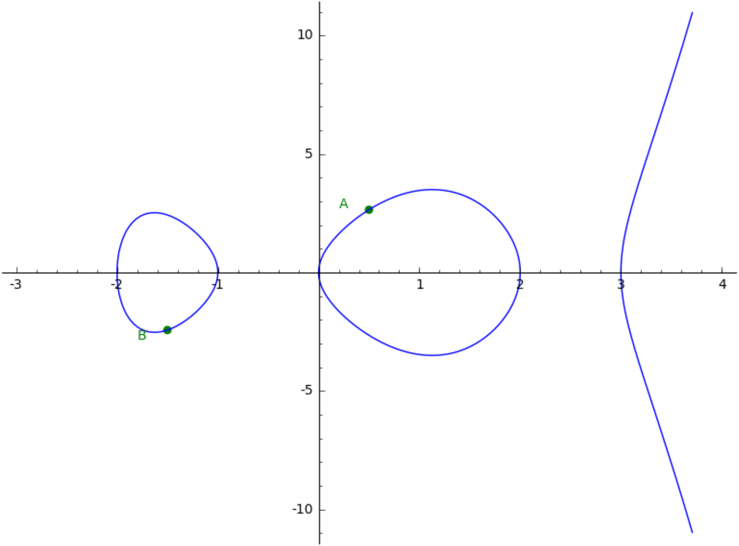
$$y^2 = f(x) \in \mathbb{F}_q[x],$$

where $\deg(f) = 5$ or 6.



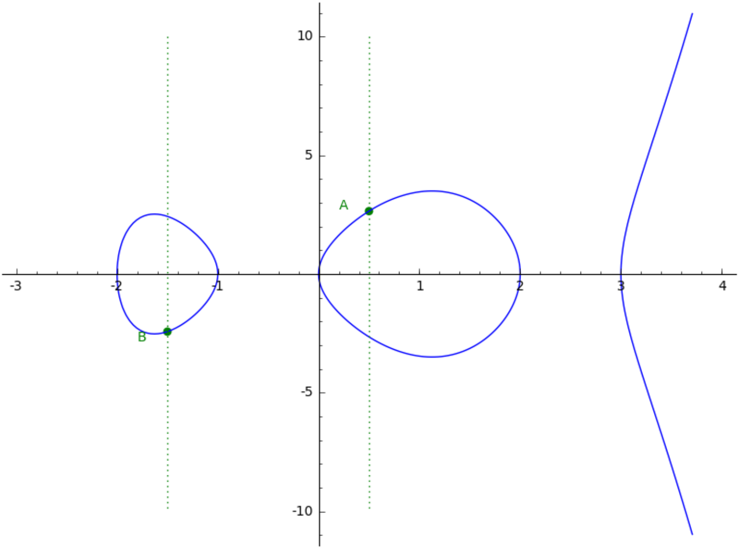
The group law for genus 2 curves

We define a group law on genus 2 curves with *pairs of points*.



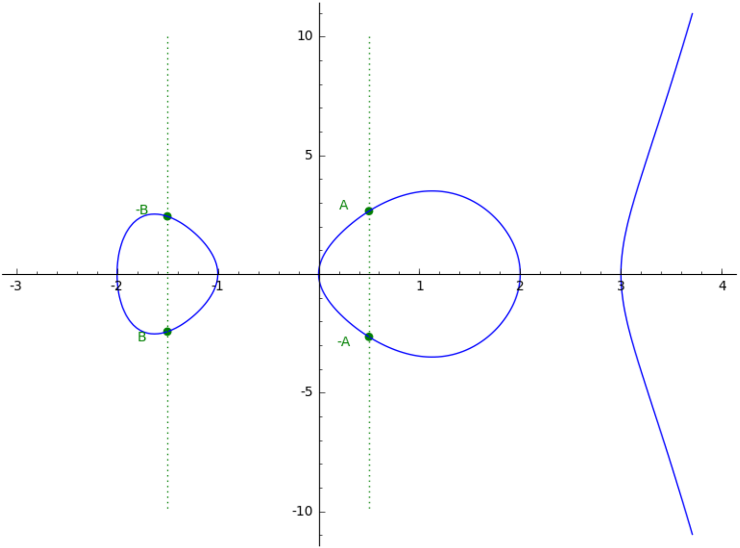
The group law for genus 2 curves

First we define the inverse of $\{A, B\}$:



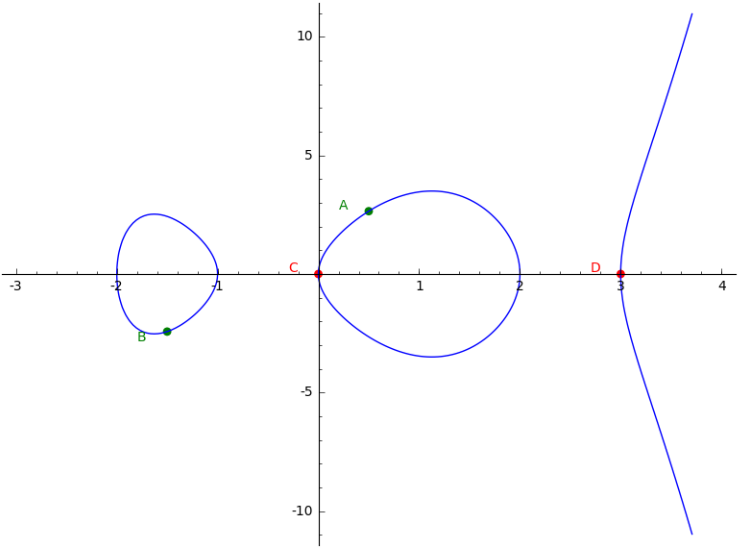
The group law for genus 2 curves

First we define the inverse of $\{A, B\}$: $-\{A, B\} = \{-A, -B\}$.



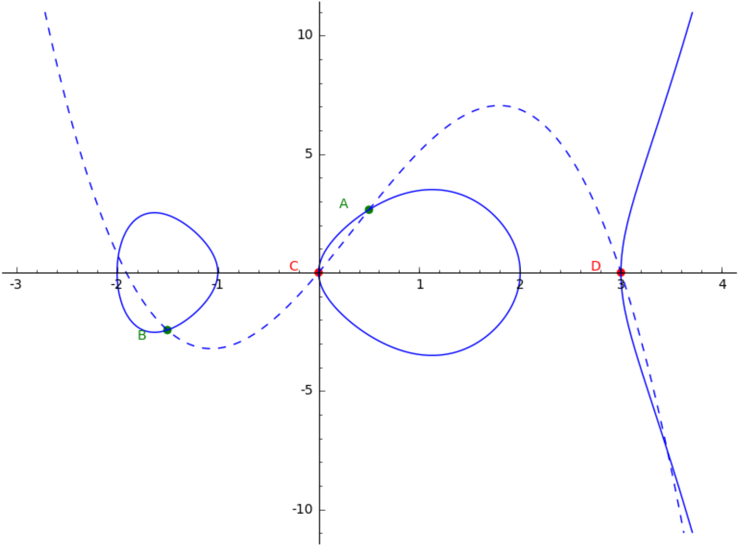
The group law for genus 2 curves

Suppose we have another pair of points $\{C, D\}$:



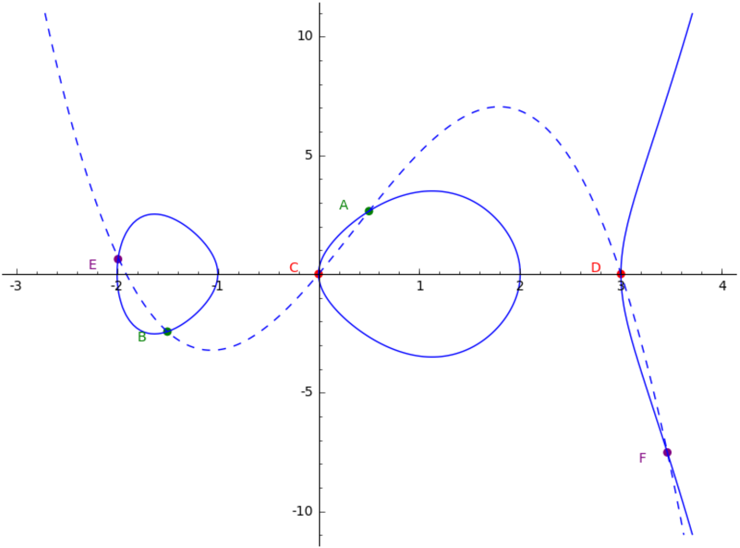
The group law for genus 2 curves

Draw the unique cubic passing through A, B, C, D:



The group law for genus 2 curves

We define $\{A, B\} + \{C, D\} + \{E, F\} = 0$.



The Frobenius for genus 2 curves

- Via this group law we can associate an abelian variety to a genus 2 curve C, called the *Jacobian of C*, or just $\mathrm{Jac}(C)$.

The Frobenius for genus 2 curves

- Via this group law we can associate an abelian variety to a genus 2 curve C, called the *Jacobian of C*, or just $\mathrm{Jac}(C)$.
- Think of points $P \in \mathrm{Jac}(C)$ as pairs of points $\{A, B\}$ on C.

The Frobenius for genus 2 curves

- Via this group law we can associate an abelian variety to a genus 2 curve C, called the *Jacobian of C*, or just $\mathrm{Jac}(C)$.
- Think of points $P \in \mathrm{Jac}(C)$ as pairs of points $\{A, B\}$ on C.

Recall:

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on E is defined to be

$$\begin{array}{rccc} \pi_q : & E & \longrightarrow & E \\ & P & \mapsto & P^q. \end{array}$$

The Frobenius for genus 2 curves

- Via this group law we can associate an abelian variety to a genus 2 curve C, called the *Jacobian of* C, or just $\mathrm{Jac}(C)$.
- Think of points $P \in \mathrm{Jac}(C)$ as pairs of points $\{A, B\}$ on C.

Recall:

Definition

Let C be an elliptic curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on E is defined to be

$$\begin{array}{rccc} \pi_q : & E & \longrightarrow & E \\ & P & \mapsto & P^q. \end{array}$$

The Frobenius for genus 2 curves

- Via this group law we can associate an abelian variety to a genus 2 curve C, called the *Jacobian of* C, or just $\mathrm{Jac}(C)$.
- Think of points $P \in \mathrm{Jac}(C)$ as pairs of points $\{A, B\}$ on C.

Recall:

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on E is defined to be

$$\begin{array}{rccc} \pi_q : & E & \longrightarrow & E \\ & P & \mapsto & P^q. \end{array}$$

The Frobenius for genus 2 curves

- Via this group law we can associate an abelian variety to a genus 2 curve C, called the *Jacobian of C*, or just $\mathrm{Jac}(C)$.
- Think of points $P \in \mathrm{Jac}(C)$ as pairs of points $\{A, B\}$ on C.

Recall:

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on $\mathrm{Jac}(C)$ is defined to be

$$\begin{array}{rccc} \pi_q : & E & \longrightarrow & E \\ & P & \mapsto & P^q. \end{array}$$

The Frobenius for genus 2 curves

- Via this group law we can associate an abelian variety to a genus 2 curve C, called the *Jacobian of C*, or just $\mathrm{Jac}(C)$.
- Think of points $P \in \mathrm{Jac}(C)$ as pairs of points $\{A, B\}$ on C.

Recall:

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on $\mathrm{Jac}(C)$ is defined to be

$$\begin{array}{rccc} \pi_q : & \mathrm{Jac}(C) & \longrightarrow & \mathrm{Jac}(C) \\ & P & \mapsto & P^q. \end{array}$$

The Frobenius for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on $\text{Jac}(C)$ is defined to be

$$\begin{array}{rccc} \pi_q : & \text{Jac}(C) & \longrightarrow & \text{Jac}(C) \\ & P & \mapsto & P^q. \end{array}$$

Recall:

- The characteristic polynomial of the Frobenius morphism on an elliptic curve is of the form

$$\chi_{\pi_q}(X) = X^2 - tX + q.$$

- $\#E(\mathbb{F}_q) = 1 - t + q$

The Frobenius for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on $\mathrm{Jac}(C)$ is defined to be

$$\begin{array}{rccc} \pi_q : & \mathrm{Jac}(C) & \longrightarrow & \mathrm{Jac}(C) \\ & P & \mapsto & P^q. \end{array}$$

Recall:

- The characteristic polynomial of the Frobenius morphism on a genus 2 curve C is of the form

$$\chi_{\pi_q}(X) = X^4 - tX^3 + (2q + s)X^2 - tqX + q^2.$$

- $\#E(\mathbb{F}_q) = 1 - t + q$

The Frobenius for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on $\text{Jac}(C)$ is defined to be

$$\begin{array}{rccc} \pi_q : & \text{Jac}(C) & \longrightarrow & \text{Jac}(C) \\ & P & \mapsto & P^q. \end{array}$$

Recall:

- The characteristic polynomial of the Frobenius morphism on a genus 2 curve C is of the form

$$\chi_{\pi_q}(X) = X^4 - tX^3 + (2q + s)X^2 - tqX + q^2.$$

- $\#C(\mathbb{F}_q) = 1 - t + q$

The Frobenius for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. The *q-power Frobenius morphism* on $\mathrm{Jac}(C)$ is defined to be

$$\begin{array}{cccc} \pi_q : & \mathrm{Jac}(C) & \longrightarrow & \mathrm{Jac}(C) \\ & P & \mapsto & P^q. \end{array}$$

Recall:

- The characteristic polynomial of the Frobenius morphism on a genus 2 curve C is of the form

$$\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2.$$

- $\#C(\mathbb{F}_q) = 1 - t + q$
- $\#\mathrm{Jac}(C)(\mathbb{F}_q) = 1 - t + 2q + s - tq + q^2$

Endomorphisms of Elliptic Curves

Definition

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. An *endomorphism* of E is defined to be a morphism $E \to E$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} E & \longrightarrow & E \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of E form a ring, called the *endomorphism ring* of E, written as $\mathrm{End}(E)$.
- To find: $E/\mathbb{F}_q$ such that $\pi \in \mathrm{End}(E)$, where

$$\chi_{\pi_q}(X) = X^2 - tX + q = (X - \pi)(X - \overline{\pi}).$$

- All such E will satisfy $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$.

Endomorphisms for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. An *endomorphism* of $\mathrm{Jac}(C)$ is defined to be a morphism $\mathrm{Jac}(C) \to \mathrm{Jac}(C)$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} E & \longrightarrow & E \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of E form a ring, called the *endomorphism ring* of E, written as $\mathrm{End}(E)$.
- To find: $E/\mathbb{F}_q$ such that $\pi \in \mathrm{End}(E)$, where

$$\chi_{\pi_q}(X) = X^2 - tX + q = (X - \pi)(X - \overline{\pi}).$$

- All such E will satisfy $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$.

Endomorphisms for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. An *endomorphism* of $\mathrm{Jac}(C)$ is defined to be a morphism $\mathrm{Jac}(C) \to \mathrm{Jac}(C)$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} \mathrm{Jac}(C) & \longrightarrow & \mathrm{Jac}(C) \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of E form a ring, called the *endomorphism ring* of E, written as $\mathrm{End}(E)$.
- To find: $E/\mathbb{F}_q$ such that $\pi \in \mathrm{End}(E)$, where

$$\chi_{\pi_q}(X) = X^2 - tX + q = (X - \pi)(X - \overline{\pi}).$$

- All such E will satisfy $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$.

Endomorphisms for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. An *endomorphism* of $\text{Jac}(C)$ is defined to be a morphism $\text{Jac}(C) \to \text{Jac}(C)$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} \text{Jac}(C) & \longrightarrow & \text{Jac}(C) \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of $\text{Jac}(C)$ form a ring, called the *endomorphism ring* of $\text{Jac}(C)$, written as $\text{End}(\text{Jac}(C))$.
- To find: $E/\mathbb{F}_q$ such that $\pi \in \text{End}(E)$, where

$$\chi_{\pi_q}(X) = X^2 - tX + q = (X - \pi)(X - \overline{\pi}).$$

- All such E will satisfy $\mathbb{Z}[\pi] \subseteq \text{End}(E)$.

Endomorphisms for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. An *endomorphism* of $\mathrm{Jac}(C)$ is defined to be a morphism $\mathrm{Jac}(C) \to \mathrm{Jac}(C)$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} \mathrm{Jac}(C) & \longrightarrow & \mathrm{Jac}(C) \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of $\mathrm{Jac}(C)$ form a ring, called the *endomorphism ring* of $\mathrm{Jac}(C)$, written as $\mathrm{End}(\mathrm{Jac}(C))$.
- To find: $C/\mathbb{F}_q$ such that $\pi \in \mathrm{End}(\mathrm{Jac}(C))$, where π is a root of $\chi_{\pi_q}(X)$.
- All such E will satisfy $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$.

Endomorphisms for genus 2 curves

Definition

Let C be a genus 2 curve over a finite field $\mathbb{F}_q$. An *endomorphism* of $\mathrm{Jac}(C)$ is defined to be a morphism $\mathrm{Jac}(C) \to \mathrm{Jac}(C)$.

Examples

- The q-power Frobenius morphism.
- $\begin{array}{ccc} \mathrm{Jac}(C) & \longrightarrow & \mathrm{Jac}(C) \\ P & \mapsto & nP, \end{array}$ where $n \in \mathbb{Z}$.

- The endomorphisms of $\mathrm{Jac}(C)$ form a ring, called the *endomorphism ring* of $\mathrm{Jac}(C)$, written as $\mathrm{End}(\mathrm{Jac}(C))$.
- To find: $C/\mathbb{F}_q$ such that $\pi \in \mathrm{End}(\mathrm{Jac}(C))$, where π is a root of $\chi_{\pi_q}(X)$.
- All such C will satisfy $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathrm{End}(\mathrm{Jac}(C))$.

Counting points on elliptic curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^2 - tX + q$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$
2. $\pi \in \mathrm{End}(E)$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$.

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is an imaginary quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$
2. $\pi \in \mathrm{End}(E)$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$.

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of a real quadratic number field.
- $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$
2. $\pi \in \mathrm{End}(E)$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$.

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of a real quadratic number field.
- $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$
2. $\pi \in \mathrm{End}(E)$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$.

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of a real quadratic number field.
- $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K = \mathrm{End}(E)$
2. $\pi \in \mathrm{End}(E)$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$.

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of a real quadratic number field.
- $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K = \mathrm{End}(\mathrm{Jac}(C))$
2. $\pi \in \mathrm{End}(E)$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$.

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of a real quadratic number field.
- $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K = \mathrm{End}(\mathrm{Jac}(C))$
2. $\pi, \overline{\pi} \in \mathrm{End}(\mathrm{Jac}(C))$
3. π defines a morphism of E with trace $\pi + \overline{\pi} = t$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$.

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of a real quadratic number field.
- $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K = \mathrm{End}(\mathrm{Jac}(C))$
2. $\pi, \overline{\pi} \in \mathrm{End}(\mathrm{Jac}(C))$
3. π defines a morphism of $\mathrm{Jac}(C)$ with characteristic polynomial $\chi_{\pi_q}(X)$ (the q-power Frobenius morphism)
4. $\#E(\mathbb{F}_q) = 1 - t + q$

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of a real quadratic number field.
- $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K = \mathrm{End}(\mathrm{Jac}(C))$
2. $\pi, \overline{\pi} \in \mathrm{End}(\mathrm{Jac}(C))$
3. π defines a morphism of $\mathrm{Jac}(C)$ with characteristic polynomial $\chi_{\pi_q}(X)$ (the q-power Frobenius morphism)
4. $\#C(\mathbb{F}_q) = 1 - t + q$

Counting points on genus 2 curves over finite fields

Suppose that π is a complex (non-real) root of $\chi_{\pi_q}(X) = X^4 - tX^3 + (2q+s)X^2 - tqX + q^2$. Then

- $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of a real quadratic number field.
- $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$ (the ring of integers of K).

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$. To recap, we then get

1. $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K = \mathrm{End}(\mathrm{Jac}(C))$
2. $\pi, \overline{\pi} \in \mathrm{End}(\mathrm{Jac}(C))$
3. π defines a morphism of $\mathrm{Jac}(C)$ with characteristic polynomial $\chi_{\pi_q}(X)$ (the q-power Frobenius morphism)
4. $\#C(\mathbb{F}_q) = 1 - t + q$
5. $\#\mathrm{Jac}(C)(\mathbb{F}_q) = 1 - t + 2q + s - tq + q^2$.

Constructing elliptic curves with a given number of points

Strategy: construct elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Definition

The *class polynomial* for K is defined to be

$$H_K(X) = \prod_{E/\mathbb{C}:\mathrm{End}(E)=\mathcal{O}_K} (X - j(E)) \in \mathbb{Z}[X].$$

- This polynomial has integral coefficients!
- The roots of $H_K(X)$ mod q are the j-invariants of all the elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
- There is an algorithm to find *all* the elliptic curves with $1 - t + q$ points given all the elliptic curves with endomorphism ring $\mathcal{O}_K$.

Interlude: Invariants of genus 2 curves

Interlude: Invariants of genus 2 curves

- The *Igusa invariants*

$$i_1, i_2, i_3 : \{C/k : C \text{ a genus 2 curve}\} \longrightarrow k$$

are functions of the coefficients of C.

Interlude: Invariants of genus 2 curves

- The *Igusa invariants*

$$i_1, i_2, i_3 : \{C/k : C \text{ a genus 2 curve}\} \longrightarrow k$$

  are functions of the coefficients of C.
- The triple $(i_1(C), i_2(C), i_3(C))$ determines $\mathrm{Jac}(C)$ up to isomorphism.

Interlude: Invariants of genus 2 curves

- The *Igusa invariants*

$$i_1, i_2, i_3 : \{C/k : C \text{ a genus 2 curve}\} \longrightarrow k$$

  are functions of the coefficients of C.
- The triple $(i_1(C), i_2(C), i_3(C))$ determines $\mathrm{Jac}(C)$ up to isomorphism.
- *Mestre's algorithm* computes C given $(i_1(C), i_2(C), i_3(C))$.

Constructing genus 2 curves with a given number of points

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

Definition

The *class polynomial* for K is defined to be

$$H_K(X) = \prod_{E/\mathbb{C}:\mathrm{End}(E)=\mathcal{O}_K} (X - j(E)) \in \mathbb{Z}[X].$$

- This polynomial has integral coefficients!
- The roots of $H_K(X)$ mod q are the j-invariants of all the elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
- There is an algorithm to find *all* the elliptic curves with $1 - t + q$ points given all the elliptic curves with endomorphism ring $\mathcal{O}_K$.

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

Definition

The *class polynomials* for K are defined to be

$$H_{K,1}(X) = \prod_{\{C/\mathbb{C}:\mathrm{End}(\mathrm{Jac}(C))=\mathcal{O}_K\}_{/\cong}} (X - i_1(C)) \in \mathbb{C}[X],$$

$$H_{K,2}(X) = \prod_{\{C/\mathbb{C}:\mathrm{End}(\mathrm{Jac}(C))=\mathcal{O}_K\}_{/\cong}} (X - i_2(C)) \in \mathbb{C}[X],$$

$$H_{K,3}(X) = \prod_{\{C/\mathbb{C}:\mathrm{End}(\mathrm{Jac}(C))=\mathcal{O}_K\}_{/\cong}} (X - i_3(C)) \in \mathbb{C}[X].$$

Constructing genus 2 curves with a given number of points

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

Definition

The *class polynomials* for K are defined to be

$$H_{K,n}(X) = \prod_{\{C/\mathbb{C}:\mathrm{End}(\mathrm{Jac}(C))=\mathcal{O}_K\}_{/\cong}} (X - i_n(C)) \in \mathbb{C}[X],$$

for $n = 1, 2, 3$.

- This polynomial has integral coefficients!
- The roots of $H_K(X)$ mod q are the j-invariants of all the elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
- There is an algorithm to find *all* the elliptic curves with $1 - t + q$ points given all the elliptic curves with endomorphism ring $\mathcal{O}_K$.

Constructing genus 2 curves with a given number of points

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

Definition

The *class polynomials* for K are defined to be

$$H_{K,n}(X) = \prod_{\{C/\mathbb{C}:\mathrm{End}(\mathrm{Jac}(C))=\mathcal{O}_K\}_{/\cong}} (X - i_n(C)) \in \mathbb{Z}[X],$$

for $n = 1, 2, 3$.

- These polynomials have integral coefficients!
- The roots of $H_K(X)$ mod q are the j-invariants of all the elliptic curves $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathcal{O}_K$.
- There is an algorithm to find *all* the elliptic curves with $1 - t + q$ points given all the elliptic curves with endomorphism ring $\mathcal{O}_K$.

Constructing genus 2 curves with a given number of points

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

Definition

The *class polynomials* for K are defined to be

$$H_{K,n}(X) = \prod_{\{C/\mathbb{C}:\mathrm{End}(\mathrm{Jac}(C))=\mathcal{O}_K\}_{/\cong}} (X - i_n(C)) \in \mathbb{Z}[X],$$

for $n = 1, 2, 3$.

- These polynomials have integral coefficients!
- The roots of $H_{K,n}(X)$ mod q are the n^{th} Igusa invariants $i_n(C)$ of all the genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.
- There is an algorithm to find *all* the elliptic curves with $1 - t + q$ points given all the elliptic curves with endomorphism ring $\mathcal{O}_K$.

Constructing genus 2 curves with a given number of points

Strategy: construct genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

Definition

The *class polynomials* for K are defined to be

$$H_{K,n}(X) = \prod_{\{C/\mathbb{C}:\mathrm{End}(\mathrm{Jac}(C))=\mathcal{O}_K\}_{/\cong}} (X - i_n(C)) \in \mathbb{Z}[X],$$

for $n = 1, 2, 3$.

- These polynomials have integral coefficients!
- The roots of $H_{K,n}(X)$ mod q are the n^{th} Igusa invariants $i_n(C)$ of all the genus 2 curves $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.
- We give an algorithm to construct many more genus 2 curves with $1 - t + q$ points given all the genus 2 curves with endomorphism ring $\mathcal{O}_K$.

Our contributions

- We give a new algorithm to compute the class polynomials for genus 2 curves that mimics the current state-of-the-art for genus 1.

Our contributions

- We give a new algorithm to compute the class polynomials for genus 2 curves that mimics the current state-of-the-art for genus 1.
- The techniques in my thesis allow us to construct many more genus 2 curves $\mathbb{F}_q$ with $N = 1 - t + q$ points than just those with maximal endomorphism ring.

Our contributions

- We give a new algorithm to compute the class polynomials for genus 2 curves that mimics the current state-of-the-art for genus 1.
- The techniques in my thesis allow us to construct many more genus 2 curves $\mathbb{F}_q$ with $N = 1 - t + q$ points than just those with maximal endomorphism ring.

Future work:

- Constructing *pairing-friendly* elliptic curves is an important research topic in cryptography.

Our contributions

- We give a new algorithm to compute the class polynomials for genus 2 curves that mimics the current state-of-the-art for genus 1.
- The techniques in my thesis allow us to construct many more genus 2 curves $\mathbb{F}_q$ with $N = 1 - t + q$ points than just those with maximal endomorphism ring.

Future work:

- Constructing *pairing-friendly* elliptic curves is an important research topic in cryptography.
- For this, we have to find an elliptic curve $E/\mathbb{F}_p$ such that $\#E(\mathbb{F}_p)$ has a prime factor r of given magnitude, and

$$k = \min\{n \in \mathbb{Z} : r | p^n - 1\}$$

is prescribed.

Our contributions

- We give a new algorithm to compute the class polynomials for genus 2 curves that mimics the current state-of-the-art for genus 1.
- The techniques in my thesis allow us to construct many more genus 2 curves $\mathbb{F}_q$ with $N = 1 - t + q$ points than just those with maximal endomorphism ring.

Future work:

- Constructing *pairing-friendly* elliptic curves is an important research topic in cryptography.
- For this, we have to find an elliptic curve $E/\mathbb{F}_p$ such that $\#E(\mathbb{F}_p)$ has a prime factor r of given magnitude, and

$$k = \min\{n \in \mathbb{Z} : r | p^n - 1\}$$

  is prescribed.
- I hope to use class polynomials to construct (families of) pairing-friendly genus 2 curves.

Thank you!