Constructing Picard curves with complex multiplication using the Chinese remainder theorem

Sonny Arora and Kirsten Eisenträger

Penn State University

July 18th, 2018

Elliptic Curves in Cryptography

- For cryptographic protocols based on the discrete log problem, one wants to find a group whose order is divisible by a large prime.

Elliptic Curves in Cryptography

- For cryptographic protocols based on the discrete log problem, one wants to find a group whose order is divisible by a large prime.
- One option: Use points on an elliptic curve or the Jacobian of a curve.

Elliptic Curves in Cryptography

- For cryptographic protocols based on the discrete log problem, one wants to find a group whose order is divisible by a large prime.
- One option: Use points on an elliptic curve or the Jacobian of a curve.

Problem

Find an elliptic curve over a finite field whose group of points has order divisible by a large prime.

Elliptic Curves in Cryptography

- For cryptographic protocols based on the discrete log problem, one wants to find a group whose order is divisible by a large prime.
- One option: Use points on an elliptic curve or the Jacobian of a curve.

Problem

Find an elliptic curve over a finite field whose group of points has order divisible by a large prime.

- This problem has been well studied and we review some approaches to this problem.

Elliptic Curves with Complex Multiplication

- Fix prime p (of cryptographic size), want elliptic curve over $\mathbb{F}_p$ with N points where N in Hasse-Weil interval.

Elliptic Curves with Complex Multiplication

- Fix prime p (of cryptographic size), want elliptic curve over $\mathbb{F}_p$ with N points where N in Hasse-Weil interval.
- E an elliptic curve over $\mathbb{F}_p$. $\#E(\mathbb{F}_p) = p + 1 - a$ where a is the trace of Frobenius of E.

Elliptic Curves with Complex Multiplication

- Fix prime p (of cryptographic size), want elliptic curve over $\mathbb{F}_p$ with N points where N in Hasse-Weil interval.
- E an elliptic curve over $\mathbb{F}_p$. $\#E(\mathbb{F}_p) = p + 1 - a$ where a is the trace of Frobenius of E.
- Fixing number of points N equivalent to fixing a trace of Frobenius. Thus, equivalent to fixing characteristic polynomial of Frobenius $x^2 - ax + p$.

Elliptic Curves with Complex Multiplication

- Fix prime p (of cryptographic size), want elliptic curve over $\mathbb{F}_p$ with N points where N in Hasse-Weil interval.
- E an elliptic curve over $\mathbb{F}_p$. $\#E(\mathbb{F}_p) = p + 1 - a$ where a is the trace of Frobenius of E.
- Fixing number of points N equivalent to fixing a trace of Frobenius. Thus, equivalent to fixing characteristic polynomial of Frobenius $x^2 - ax + p$.
- If $a \not\equiv 0 \mod p$, then E is ordinary and has endomorphism ring an order in the imaginary quadratic field $\mathbb{Q}(\pi)$ where π is a root of $x^2 - ax + p$.

Elliptic Curves with Complex Multiplication

- Fix prime p (of cryptographic size), want elliptic curve over $\mathbb{F}_p$ with N points where N in Hasse-Weil interval.
- E an elliptic curve over $\mathbb{F}_p$. $\#E(\mathbb{F}_p) = p + 1 - a$ where a is the trace of Frobenius of E.
- Fixing number of points N equivalent to fixing a trace of Frobenius. Thus, equivalent to fixing characteristic polynomial of Frobenius $x^2 - ax + p$.
- If $a \not\equiv 0 \mod p$, then E is ordinary and has endomorphism ring an order in the imaginary quadratic field $\mathbb{Q}(\pi)$ where π is a root of $x^2 - ax + p$.
- When End(E) contains an order in a quadratic imaginary field, we say that E has **Complex Multiplication** (CM).

Elliptic Curves with Complex Multiplication

- Fix prime p (of cryptographic size), want elliptic curve over $\mathbb{F}_p$ with N points where N in Hasse-Weil interval.
- E an elliptic curve over $\mathbb{F}_p$. $\#E(\mathbb{F}_p) = p + 1 - a$ where a is the trace of Frobenius of E.
- Fixing number of points N equivalent to fixing a trace of Frobenius. Thus, equivalent to fixing characteristic polynomial of Frobenius $x^2 - ax + p$.
- If $a \not\equiv 0 \mod p$, then E is ordinary and has endomorphism ring an order in the imaginary quadratic field $\mathbb{Q}(\pi)$ where π is a root of $x^2 - ax + p$.
- When $\mathrm{End}(E)$ contains an order in a quadratic imaginary field, we say that E has **Complex Multiplication** (CM).
- Given an ordinary elliptic curve E with CM by K then (up to a twist) E has N points.

Constructing Elliptic Curves with CM

- Suffices to solve the following:

Constructing Elliptic Curves with CM

- Suffices to solve the following:
- **Problem:** Given K an imaginary quadratic field, construct an ordinary elliptic curve over $\mathbb{F}_p$ which has Complex Multiplication (CM) by $\mathcal{O}_K$.

Constructing Elliptic Curves with CM

- Suffices to solve the following:
- **Problem:** Given K an imaginary quadratic field, construct an ordinary elliptic curve over $\mathbb{F}_p$ which has Complex Multiplication (CM) by $\mathcal{O}_K$.
- Idea: Find elliptic curves with CM by $\mathcal{O}_K$ over $\mathbb{C}$ and reduce them modulo p.

Constructing Elliptic Curves with CM

- Suffices to solve the following:
- **Problem:** Given K an imaginary quadratic field, construct an ordinary elliptic curve over $\mathbb{F}_p$ which has Complex Multiplication (CM) by $\mathcal{O}_K$.
- Idea: Find elliptic curves with CM by $\mathcal{O}_K$ over $\mathbb{C}$ and reduce them modulo p.

Definition

For K a quadratic imaginary number field, the **Hilbert class polynomial** H_K with respect to K is a polynomial that has as roots the j-invariants of all elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}_K$.

Constructing Elliptic Curves with CM

- Suffices to solve the following:
- **Problem:** Given K an imaginary quadratic field, construct an ordinary elliptic curve over $\mathbb{F}_p$ which has Complex Multiplication (CM) by $\mathcal{O}_K$.
- Idea: Find elliptic curves with CM by $\mathcal{O}_K$ over $\mathbb{C}$ and reduce them modulo p.

Definition

For K a quadratic imaginary number field, the **Hilbert class polynomial** H_K with respect to K is a polynomial that has as roots the j-invariants of all elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}_K$.

Approach

- Compute the Hilbert class polynomial H_K.

Constructing Elliptic Curves with CM

- Suffices to solve the following:
- **Problem:** Given K an imaginary quadratic field, construct an ordinary elliptic curve over $\mathbb{F}_p$ which has Complex Multiplication (CM) by $\mathcal{O}_K$.
- Idea: Find elliptic curves with CM by $\mathcal{O}_K$ over $\mathbb{C}$ and reduce them modulo p.

Definition

For K a quadratic imaginary number field, the **Hilbert class polynomial** H_K with respect to K is a polynomial that has as roots the j-invariants of all elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}_K$.

Approach

- Compute the Hilbert class polynomial H_K.
- Reduce H_K modulo p.

Constructing Elliptic Curves with CM

- Suffices to solve the following:
- **Problem:** Given K an imaginary quadratic field, construct an ordinary elliptic curve over $\mathbb{F}_p$ which has Complex Multiplication (CM) by $\mathcal{O}_K$.
- Idea: Find elliptic curves with CM by $\mathcal{O}_K$ over $\mathbb{C}$ and reduce them modulo p.

Definition

For K a quadratic imaginary number field, the **Hilbert class polynomial** H_K with respect to K is a polynomial that has as roots the j-invariants of all elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}_K$.

Approach

- Compute the Hilbert class polynomial H_K.
- Reduce H_K modulo p.
- Root of H_K modulo p gives j-invariant of curve with CM by $\mathcal{O}_K$, if p satisfies certain condition.

Computing the Hilbert class polynomial: CRT Approach

CRT Approach due to Agashe-Lauter-Venkatesan and others:

- Hilbert class polynomial has integer coefficients.

Computing the Hilbert class polynomial: CRT Approach

CRT Approach due to Agashe-Lauter-Venkatesan and others:

- Hilbert class polynomial has integer coefficients.
- One method:

Computing the Hilbert class polynomial: CRT Approach

CRT Approach due to Agashe-Lauter-Venkatesan and others:

- Hilbert class polynomial has integer coefficients.
- One method:
  1. Compute for several small primes ℓ_j satisfying certain conditions:

$$H_K \mod \ell_j$$

Computing the Hilbert class polynomial: CRT Approach

CRT Approach due to Agashe-Lauter-Venkatesan and others:

- Hilbert class polynomial has integer coefficients.
- One method:
  1. Compute for several small primes ℓ_j satisfying certain conditions:
  $$H_K \mod \ell_j$$
  2. Use the Chinese Remainder Theorem (CRT) to reconstruct H_K from $H_K \mod \ell_j$.

Computing the Hilbert class polynomial: CRT Approach

CRT Approach due to Agashe-Lauter-Venkatesan and others:

- Hilbert class polynomial has integer coefficients.
- One method:
  1. Compute for several small primes ℓ_j satisfying certain conditions:
  $$H_K \mod \ell_j$$
  2. Use the Chinese Remainder Theorem (CRT) to reconstruct H_K from $H_K \mod \ell_j$.
- Step 1) involves enumerating all isomorphism classes of elliptic curves E defined over $\mathbb{F}_{\ell_j}$ and determining if the endomorphism ring of E is $\mathcal{O}_K$.

Computing the Hilbert class polynomial: CRT Approach

CRT Approach due to Agashe-Lauter-Venkatesan and others:

- Hilbert class polynomial has integer coefficients.
- One method:
  1. Compute for several small primes ℓ_j satisfying certain conditions:
     $$H_K \mod \ell_j$$
  2. Use the Chinese Remainder Theorem (CRT) to reconstruct H_K from $H_K \mod \ell_j$.
- Step 1) involves enumerating all isomorphism classes of elliptic curves E defined over $\mathbb{F}_{\ell_j}$ and determining if the endomorphism ring of E is $\mathcal{O}_K$.
- Step 2) involves using a bound on the coefficients of H_K.

Computing the Hilbert class polynomial: CRT Approach

- CRT method heuristically has the same running time as two other main approaches: The Complex Analytic and the p-adic approach.
- Several improvements to CRT method: Belding-Bröker-Enge-Lauter, Sutherland-Enge, Sutherland and others.
- Largest known examples of Hilbert class polynomials modulo a prime have been computed using a CRT approach.

Higher Genus

Problem

For a given CM-field K of degree $2g$, construct curves C of genus g over a finite field $\mathbb{F}_p$ whose Jacobian is ordinary and $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$.

Higher Genus

Problem

For a given CM-field K of degree $2g$, construct curves C of genus g over a finite field $\mathbb{F}_p$ whose Jacobian is ordinary and $\text{End}(\text{Jac}(C)) \cong \mathcal{O}_K$.

Definition

A CM-field is a totally imaginary quadratic extension of a totally real number field.

Higher Genus

Problem

For a given CM-field K of degree $2g$, construct curves C of genus g over a finite field $\mathbb{F}_p$ whose Jacobian is ordinary and $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$.

Definition

A CM-field is a totally imaginary quadratic extension of a totally real number field.

Example

$n > 2$, $\mathbb{Q}(\zeta_n)$ is a totally imaginary quadratic extension of the totally real field $\mathbb{Q}(\zeta_n + \overline{\zeta_n})$ where ζ_n is an n-th root of unity. Thus, it is a CM-field.

Higher Genus

Problem

For a given CM-field K of degree $2g$, construct curves C of genus g over a finite field $\mathbb{F}_p$ whose Jacobian is ordinary and $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$.

Definition

A CM-field is a totally imaginary quadratic extension of a totally real number field.

Example

$n > 2$, $\mathbb{Q}(\zeta_n)$ is a totally imaginary quadratic extension of the totally real field $\mathbb{Q}(\zeta_n + \overline{\zeta_n})$ where ζ_n is an n-th root of unity. Thus, it is a CM-field.

Definition

An abelian variety A **has CM by** K if there exists an embedding $\iota : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$. If $\iota^{-1}(\mathrm{End}(A)) = \mathcal{O}$ for $\mathcal{O}$ an order of K, then, we say that A has CM by $\mathcal{O}$.

Genus 2

- Every genus 2 curve is hyperelliptic.

Genus 2

- Every genus 2 curve is hyperelliptic.
- Analogue of j-invariant for genus 2 curves: triple of Igusa invariants (j_1, j_2, j_3).

Genus 2

- Every genus 2 curve is hyperelliptic.
- Analogue of j-invariant for genus 2 curves: triple of Igusa invariants (j_1, j_2, j_3).
- Analogue of quadratic imaginary field: Quartic CM-field.

Genus 2

- Every genus 2 curve is hyperelliptic.
- Analogue of j-invariant for genus 2 curves: triple of Igusa invariants (j_1, j_2, j_3).
- Analogue of quadratic imaginary field: Quartic CM-field.
- Analogue of Hilbert class polynomials: **Three** Igusa class polynomials which have rational coefficients.

Genus 2

- Every genus 2 curve is hyperelliptic.
- Analogue of j-invariant for genus 2 curves: triple of Igusa invariants (j_1, j_2, j_3).
- Analogue of quadratic imaginary field: Quartic CM-field.
- Analogue of Hilbert class polynomials: **Three** Igusa class polynomials which have rational coefficients.
- Several methods to construct curves whose Jacobian have complex multiplication.

Genus 2

- Every genus 2 curve is hyperelliptic.
- Analogue of j-invariant for genus 2 curves: triple of Igusa invariants (j_1, j_2, j_3).
- Analogue of quadratic imaginary field: Quartic CM-field.
- Analogue of Hilbert class polynomials: **Three** Igusa class polynomials which have rational coefficients.
- Several methods to construct curves whose Jacobian have complex multiplication.
- Work of Eisenträger-Lauter, Freeman-Lauter presented a CRT approach to constructing genus 2 curves. Improvements made by Lauter-Robert.

Genus 3

Goal

For a a sextic CM field K, construct genus 3 curves C with $\mathrm{Jac}(C)$ ordinary and $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$.

Genus 3

Goal

For a a sextic CM field K, construct genus 3 curves C with $\mathrm{Jac}(C)$ ordinary and $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$.

- Genus 3 curves are either hyperelliptic or smooth plane quartics.

Genus 3

Goal

For a a sextic CM field K, construct genus 3 curves C with $\mathrm{Jac}(C)$ ordinary and $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$.

- Genus 3 curves are either hyperelliptic or smooth plane quartics.
- Invariants exist for each class of curves respectively, however, no invariants are known for the entire class of genus 3 curves.

Genus 3

Goal

For a a sextic CM field K, construct genus 3 curves C with $\mathrm{Jac}(C)$ ordinary and $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$.

- Genus 3 curves are either hyperelliptic or smooth plane quartics.
- Invariants exist for each class of curves respectively, however, no invariants are known for the entire class of genus 3 curves.
- Restrict to a certain class of genus 3 curves called Picard curves which have a good invariant theory.

Genus 3

Goal

For a a sextic CM field K, construct genus 3 curves C with $\text{Jac}(C)$ ordinary and $\text{End}(\text{Jac}(C)) \cong \mathcal{O}_K$.

- Genus 3 curves are either hyperelliptic or smooth plane quartics.
- Invariants exist for each class of curves respectively, however, no invariants are known for the entire class of genus 3 curves.
- Restrict to a certain class of genus 3 curves called Picard curves which have a good invariant theory.
- Need a restriction on sextic CM-field K so that all curves with CM by $\mathcal{O}_K$ are Picard curves.

Picard Curves

Definition

A Picard curve is a curve of the form $y^3 = f(x)$ over a field k of characteristic not 2 or 3 where f is a degree 4 polynomial with has no repeated roots over the algebraic closure of k.

Picard Curves

Definition

A Picard curve is a curve of the form $y^3 = f(x)$ over a field k of characteristic not 2 or 3 where f is a degree 4 polynomial with has no repeated roots over the algebraic closure of k.

- Koike and Weng show that if K is a sextic CM-field with $\mathbb{Q}(\zeta_3) \subset K$, then every curve $C/\mathbb{C}$ such that $\mathrm{Jac}(C)$ has CM by $\mathcal{O}_K$ is (geometrically) a Picard curve. So will only consider such fields.

Picard Curves

Definition

A Picard curve is a curve of the form $y^3 = f(x)$ over a field k of characteristic not 2 or 3 where f is a degree 4 polynomial with has no repeated roots over the algebraic closure of k.

- Koike and Weng show that if K is a sextic CM-field with $\mathbb{Q}(\zeta_3) \subset K$, then every curve $C/\mathbb{C}$ such that $\mathrm{Jac}(C)$ has CM by $\mathcal{O}_K$ is (geometrically) a Picard curve. So will only consider such fields.
- For a CRT approach to constructing Picard curves, one must first define suitable invariants.

Picard Curves

Definition

A Picard curve is a curve of the form $y^3 = f(x)$ over a field k of characteristic not 2 or 3 where f is a degree 4 polynomial with has no repeated roots over the algebraic closure of k.

- Koike and Weng show that if K is a sextic CM-field with $\mathbb{Q}(\zeta_3) \subset K$, then every curve $C/\mathbb{C}$ such that $\mathrm{Jac}(C)$ has CM by $\mathcal{O}_K$ is (geometrically) a Picard curve. So will only consider such fields.
- For a CRT approach to constructing Picard curves, one must first define suitable invariants.
- Use the invariants j_1, j_2, j_3 for a Picard curve C whose Jacobian is simple. These are defined in Kılıçer-García-Streng

Picard Curves

Definition

A Picard curve is a curve of the form $y^3 = f(x)$ over a field k of characteristic not 2 or 3 where f is a degree 4 polynomial with has no repeated roots over the algebraic closure of k.

- Koike and Weng show that if K is a sextic CM-field with $\mathbb{Q}(\zeta_3) \subset K$, then every curve $C/\mathbb{C}$ such that $\mathrm{Jac}(C)$ has CM by $\mathcal{O}_K$ is (geometrically) a Picard curve. So will only consider such fields.
- For a CRT approach to constructing Picard curves, one must first define suitable invariants.
- Use the invariants j_1, j_2, j_3 for a Picard curve C whose Jacobian is simple. These are defined in Kılıçer-García-Streng
- To define class polynomials, need notion of CM-type.

CM-types

Definition

Let K be a CM-field. Let ρ denote complex conjugation on K. Then, any subset of the embeddings Φ that satisfies $\Phi \sqcup \rho \circ \Phi = \mathrm{Hom}(K, \mathbb{C})$ is called a **CM-type** on K.

CM-types

Definition

Let K be a CM-field. Let ρ denote complex conjugation on K. Then, any subset of the embeddings Φ that satisfies $\Phi \sqcup \rho \circ \Phi = \mathrm{Hom}(K, \mathbb{C})$ is called a **CM-type** on K.

- For A an abelian variety over $\mathbb{C}$ of dimension g with CM by K of degree $2g$ over $\mathbb{Q}$, if $\iota : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$ then we can associate to (A, ι) a CM-type Φ.

CM-types

Definition

Let K be a CM-field. Let ρ denote complex conjugation on K. Then, any subset of the embeddings Φ that satisfies $\Phi \sqcup \rho \circ \Phi = \mathrm{Hom}(K, \mathbb{C})$ is called a **CM-type** on K.

- For A an abelian variety over $\mathbb{C}$ of dimension g with CM by K of degree $2g$ over $\mathbb{Q}$, if $\iota : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$ then we can associate to (A, ι) a CM-type Φ.

Definition

With assumptions as above, we say that an abelian variety A over $\mathbb{C}$ with CM by K **has CM-type** Φ if there exists an embedding $\iota : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$ such that Φ is the unique CM-type associated to (A, ι).

Class Polynomials

- For fixed primitive CM-type Φ, define class polynomials defined over $\mathbb{Q}$ for $i = 1, 2, 3$ as follows:

$$H_i := H_i^{(K,\Phi)} := \prod (X - j_i(C))$$

where the product runs over all isomorphism classes of curves whose Jacobian has CM by $\mathcal{O}_K$ and type $\sigma\Phi$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Class Polynomials

- For fixed primitive CM-type Φ, define class polynomials defined over $\mathbb{Q}$ for $i = 1, 2, 3$ as follows:

$$H_i := H_i^{(K,\Phi)} := \prod (X - j_i(C))$$

  where the product runs over all isomorphism classes of curves whose Jacobian has CM by $\mathcal{O}_K$ and type $\sigma\Phi$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- Coefficients can have denominators. For CRT we need to clear denominators.

Class Polynomials

- For fixed primitive CM-type Φ, define class polynomials defined over $\mathbb{Q}$ for $i = 1, 2, 3$ as follows:

$$H_i := H_i^{(K,\Phi)} := \prod (X - j_i(C))$$

  where the product runs over all isomorphism classes of curves whose Jacobian has CM by $\mathcal{O}_K$ and type $\sigma\Phi$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- Coefficients can have denominators. For CRT we need to clear denominators.
- Recall, if K is a sextic CM-field with $\mathbb{Q}(\zeta_3) \subset K$, all principally polarized abelian varieties with CM by $\mathcal{O}_K$ are Jacobians of Picard curves.

Main Theorem

Theorem (A.-Eisenträger)

Let K be a sextic CM-field with $\mathbb{Q}(\zeta_3) \subset K$. On input a bound B on the denominators of the coefficients of class polynomials H_i and a bound M on the size of the coefficients, we construct the polynomials H_i for $i = 1, 2, 3$ using a CRT approach. In particular, this gives an algorithm to construct Picard curves over $\mathbb{F}_p$ with complex multiplication by $\mathcal{O}_K$.

Idea of Proof of Theorem

- Multiply H_i by B to clear denominators

Idea of Proof of Theorem

- Multiply H_i by B to clear denominators
  1. Compute for several small primes ℓ_j:

$$B \cdot H_i \mod \ell_j$$

Idea of Proof of Theorem

- Multiply H_i by B to clear denominators
  1. Compute for several small primes ℓ_j:

$$B \cdot H_i \mod \ell_j$$

  2. Use the Chinese Remainder Theorem (CRT) to reconstruct $B \cdot H_i$ from $B \cdot H_i \mod \ell_j$.

Idea of Proof of Theorem

- Multiply H_i by B to clear denominators
  1. Compute for several small primes ℓ_j:
  $$B \cdot H_i \mod \ell_j$$
  2. Use the Chinese Remainder Theorem (CRT) to reconstruct $B \cdot H_i$ from $B \cdot H_i \mod \ell_j$.
- Step 1):

Idea of Proof of Theorem

- Multiply H_i by B to clear denominators
  1. Compute for several small primes ℓ_j:
  $$B \cdot H_i \mod \ell_j$$
  2. Use the Chinese Remainder Theorem (CRT) to reconstruct $B \cdot H_i$ from $B \cdot H_i \mod \ell_j$.
- Step 1):
  - Determine conditions on primes ℓ_j for good reduction properties.

Idea of Proof of Theorem

- Multiply H_i by B to clear denominators
  1. Compute for several small primes ℓ_j:
     $$B \cdot H_i \mod \ell_j$$
  2. Use the Chinese Remainder Theorem (CRT) to reconstruct $B \cdot H_i$ from $B \cdot H_i \mod \ell_j$.
- Step 1):
  - Determine conditions on primes ℓ_j for good reduction properties.
  - Need one-to-one correspondence of curves over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type Φ and computable set of curves over $\mathbb{F}_p$. This involves the Taniyama-Shimura congruence relation which relates the type of an abelian variety to the Frobenius of its reduction.

Idea of Proof of Theorem

- Multiply H_i by B to clear denominators
  1. Compute for several small primes ℓ_j:
  $$B \cdot H_i \mod \ell_j$$
  2. Use the Chinese Remainder Theorem (CRT) to reconstruct $B \cdot H_i$ from $B \cdot H_i \mod \ell_j$.
- Step 1):
  - Determine conditions on primes ℓ_j for good reduction properties.
  - Need one-to-one correspondence of curves over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type Φ and computable set of curves over $\mathbb{F}_p$. This involves the Taniyama-Shimura congruence relation which relates the type of an abelian variety to the Frobenius of its reduction.
  - Need genus 3 algorithm for determining if endomorphism ring is $\mathcal{O}_K$. Generalizes algorithm in genus 2.

Bounds on Denominators of Coefficients of Class Polynomials

- Genus 2: Bound on denominators of coefficients of Igusa class polynomials: Goren-Lauter, Bruinier-Yang, Yang, Lauter-Viray and others.

Bounds on Denominators of Coefficients of Class Polynomials

- Genus 2: Bound on denominators of coefficients of Igusa class polynomials: Goren-Lauter, Bruinier-Yang, Yang, Lauter-Viray and others.
- Genus 3: Bound on primes occurring in denominators of class polynomials presented for hyperelliptic curves and Picard curves through work of Bouw-Cooley-Lauter-Garcia-Manes-Newton-Ozman and Kılıçer-Lauter-Garcia-Newton-Ozman-Streng.

Bounds on Denominators of Coefficients of Class Polynomials

- Genus 2: Bound on denominators of coefficients of Igusa class polynomials: Goren-Lauter, Bruinier-Yang, Yang, Lauter-Viray and others.
- Genus 3: Bound on primes occurring in denominators of class polynomials presented for hyperelliptic curves and Picard curves through work of Bouw-Cooley-Lauter-Garcia-Manes-Newton-Ozman and Kılıçer-Lauter-Garcia-Newton-Ozman-Streng.
- Bound on powers to which primes occur in the denominators of class polynomials for genus 3 still open.

Examples

Example 1:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.

Examples

Example 1:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.

Examples

Example 1:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.
- Set $K = K^+(\zeta_3)$. K is a sextic CM-field.

Examples

Example 1:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.
- Set $K = K^+(\zeta_3)$. K is a sextic CM-field.
- Smallest primes satisfying conditions for CRT are $13, 43, 97, 127$.
- Over $\mathbb{F}_{127}$, our algorithm finds one Picard curve C with $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$:

$$y^3 = x^4 + 75x^2 + 37x + 103$$

Examples

Example 1:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.
- Set $K = K^+(\zeta_3)$. K is a sextic CM-field.
- Smallest primes satisfying conditions for CRT are $13, 43, 97, 127$.
- Over $\mathbb{F}_{127}$, our algorithm finds one Picard curve C with $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$:

$$y^3 = x^4 + 75x^2 + 37x + 103$$

- All Picard curves over $\mathbb{C}$ (there is only one) with CM by $\mathcal{O}_K$ as above were computed in work of Koike-Weng.

Examples

Example 1:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.
- Set $K = K^+(\zeta_3)$. K is a sextic CM-field.
- Smallest primes satisfying conditions for CRT are $13, 43, 97, 127$.
- Over $\mathbb{F}_{127}$, our algorithm finds one Picard curve C with $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$:

$$y^3 = x^4 + 75x^2 + 37x + 103$$

- All Picard curves over $\mathbb{C}$ (there is only one) with CM by $\mathcal{O}_K$ as above were computed in work of Koike-Weng.
- Our output agrees with the result of their paper reduced modulo 127.

Examples

Example 1:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.
- Set $K = K^+(\zeta_3)$. K is a sextic CM-field.
- Smallest primes satisfying conditions for CRT are $13, 43, 97, 127$.
- Over $\mathbb{F}_{127}$, our algorithm finds one Picard curve C with $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$:

$$y^3 = x^4 + 75x^2 + 37x + 103$$

- All Picard curves over $\mathbb{C}$ (there is only one) with CM by $\mathcal{O}_K$ as above were computed in work of Koike-Weng.
- Our output agrees with the result of their paper reduced modulo 127.
- Our algorithm took 7 Hours and 9 minutes of clock time.

Examples

Example 1 (continued):

- For K as in previous slide. Given we know

$$C : y^3 = x^4 - 7^2 \cdot 2x^2 + 7^2 \cdot 2^3 - 7^3$$

is the only Picard curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$.

Examples

Example 1 (continued):

- For K as in previous slide. Given we know

$$C : y^3 = x^4 - 7^2 \cdot 2x^2 + 7^2 \cdot 2^3 - 7^3$$

  is the only Picard curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$.
- Construct class polynomials H_i, $i = 1, 2, 3$.

Examples

Example 1 (continued):

- For K as in previous slide. Given we know

$$C : y^3 = x^4 - 7^2 \cdot 2x^2 + 7^2 \cdot 2^3 - 7^3$$

is the only Picard curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$.

- Construct class polynomials H_i, $i = 1, 2, 3$.
- Compute bounds B and M for theorem. $B = 2^{12}$, $M = 7$ work.

Example 1 (continued):

- For K as in previous slide. Given we know

$$C : y^3 = x^4 - 7^2 \cdot 2x^2 + 7^2 \cdot 2^3 - 7^3$$

  is the only Picard curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$.
- Construct class polynomials H_i, $i = 1, 2, 3$.
- Compute bounds B and M for theorem. $B = 2^{12}$, $M = 7$ work.
- Need 4 primes for CRT: $13, 43, 97, 127$.

Examples

Example 1 (continued):

- For K as in previous slide. Given we know

$$C : y^3 = x^4 - 7^2 \cdot 2x^2 + 7^2 \cdot 2^3 - 7^3$$

  is the only Picard curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$.
- Construct class polynomials H_i, $i = 1, 2, 3$.
- Compute bounds B and M for theorem. $B = 2^{12}$, $M = 7$ work.
- Need 4 primes for CRT: $13, 43, 97, 127$.
- Construct class polynomials using CRT algorithm in 8 hours 55 minutes of clock time.

Examples

Example 1 (continued):

- For K as in previous slide. Given we know

$$C : y^3 = x^4 - 7^2 \cdot 2x^2 + 7^2 \cdot 2^3 - 7^3$$

is the only Picard curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$.

- Construct class polynomials H_i, $i = 1, 2, 3$.
- Compute bounds B and M for theorem. $B = 2^{12}$, $M = 7$ work.
- Need 4 primes for CRT: $13, 43, 97, 127$.
- Construct class polynomials using CRT algorithm in 8 hours 55 minutes of clock time.
- Output agrees with example computed by Koike-Weng.

Examples

Example 2:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.

Examples

Example 2:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.

Examples

Example 2:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.
- Set $K = K^+(\zeta_3)$. K is a sextic CM-field.

Examples

Example 2:

- K^+ be generated by a root of $y^3 - y^2 - 2y + 1$ over $\mathbb{Q}$.
- K^+ totally real cubic extension of $\mathbb{Q}$.
- Set $K = K^+(\zeta_3)$. K is a sextic CM-field.
- Smallest prime satisfying conditions for CRT: 67.
- Over $\mathbb{F}_{67}$, our algorithm finds three ordinary, Picard curves with CM by $\mathcal{O}_K$.
  $y^3 = x^4 + 8x^2 + 64x + 61, \quad y^3 = x^4 + 62x^2 + 25x + 6, \quad y^3 = x^4 + 54x + 54.$