Constructing genus 2 curves over finite fields

Kirsten Eisenträger

The Pennsylvania State University

Fq12, Saratoga Springs

July 15, 2015

Curves and cryptography

RSA: most widely used public key cryptosystem.
Hardness assumption:

- Factoring is hard.
- Given $N = p \cdot q$ for two secret primes p and q, hard to find p, q.

Elliptic and hyperelliptic curve cryptography: alternative to RSA.
Advantage: smaller key size than RSA.

- have associated abelian groups.
- want to control the group order.

Hardness assumption: discrete log problem on the associated groups is hard.

Main Result: curves with a prescribed number of points

This talk: joint work with Kristin Lauter (2009).
Give an algorithm for the following problem (under certain conditions):

Problem: Given (ℓ, N_1, N_2) with ℓ prime and N_1, N_2 positive integers:
Construct a genus 2 curve C over $\mathbb{F}_\ell$ such that

$$\#C(\mathbb{F}_\ell) = N_1 \text{ and } \#C(\mathbb{F}_{\ell^2}) = N_2.$$

For cryptographic applications: want to choose N_1, N_2 so that the number of points on the *Jacobian* of the curve C is prime.

Overview of Talk

Part 1: Elliptic curves

- Explain use of elliptic curves in cryptography.
- Elliptic curves: easier case.
- For elliptic curves: problem reduces to computing *Hilbert class polynomials*. Explain CRT algorithm for computing them.

Part 2: Genus 2 curves

- Generalize to genus 2 curves.
- Show that the problem reduces to computing Igusa class polynomials. Give an algorithm for computing them.

Part 1
Using elliptic curves for cryptography

In 1985: N. Koblitz and V. Miller suggested using elliptic curves for cryptography.

- Approach uses the group structure of elliptic curves over finite fields.
- For crypto: want curves E over a field $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p)$ is prime.
- Hardness assumption: discrete log problem on an elliptic curve is hard.

Elliptic Curves

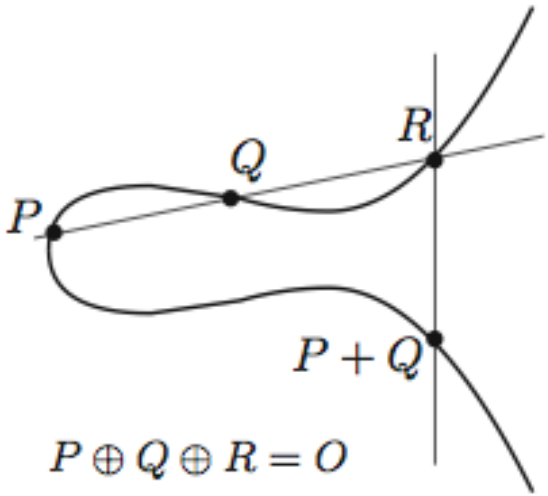
- Over a field K of characteristic $\neq 2$, consider the curve

$$E : y^2 = x^3 + ax + b, \tag{1}$$

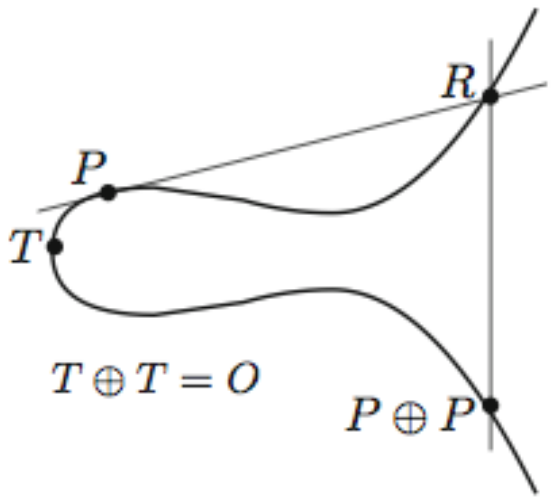
  with $a, b \in K$ and s.t. $x^3 + ax + b$ has no repeated roots.
- Then E is an *elliptic curve*.
- Denote by $E(K)$ the points (x, y) on E with coordinates in K, together with the point at infinity.
- $E(K)$ is an abelian group.

The group law on elliptic curves

- Group law is given by equations. The point at infinity is the identity element of the group.
- Also have geometric interpretation of the group law:



Addition of distinct points



Adding a point to itself

Properties of elliptic curves over finite fields

Let ℓ be a prime. Let E be an elliptic curve defined over $\mathbb{F}_\ell$.

- $\#E(\mathbb{F}_\ell) \in [\ell + 1 - 2\sqrt{\ell}, \ell + 1 + 2\sqrt{\ell}]$.
- Frobenius endomorphism π is an element of the endomorphism ring $\mathrm{End}(E)$.

  $\pi : (x, y) \mapsto (x^\ell, y^\ell)$.

  Characteristic polynomial of π: $X^2 - tX + \ell$, where t is the trace of Frobenius.

  So π is an element of $\mathbb{Q}(\sqrt{D})$ with $D = t^2 - 4\ell$.
- Can show: when the trace of π is nonzero mod ℓ, then $\mathrm{End}(E)$ is an order in $\mathbb{Q}(\sqrt{D})$ and $D < 0$.

Elliptic curves with prescribed group order

GOAL: Let ℓ be a prime. Given

$$N \in [\ell + 1 - 2\sqrt{\ell}, \ell + 1 + 2\sqrt{\ell}],$$

construct elliptic curve $E_0/\mathbb{F}_\ell$ with $\#E_0(\mathbb{F}_\ell) = N$.

- Know: $\#E_0(\mathbb{F}_\ell) = N = \ell + 1 - t$ where t is the trace of the Frobenius endomorphism π of E_0 over $\mathbb{F}_\ell$. Assume $t \not\equiv 0$.
- Since $t \not\equiv 0 \bmod \ell$, $\mathrm{End}(E_0)$ is an order in $K := \mathbb{Q}(\sqrt{D})$ with $D = t^2 - 4\ell$.
- Approach to construct E_0: Find elliptic curve E defined over a number field with $\mathrm{End}(E) = \mathcal{O}_K$ and reduce it modulo ℓ.

Approach for finding elliptic curves with prescribed group order

GOAL: Given ℓ, N as above: construct elliptic curve $E_0/\mathbb{F}_\ell$ with $\#E_0(\mathbb{F}_\ell) = N$.

Algorithm Sketch:

- Let π be the Frobenius endomorphism of E_0, t its trace ($\not\equiv 0$), and $D = t^2 - 4\ell$. Let $K := \mathbb{Q}(\sqrt{D})$.
- Compute *Hilbert class polynomial* $H_D(X)$ of K.
- Let j_0 be a root of H_D modulo ℓ. Take curve $E_0/\mathbb{F}_\ell$ with *j-invariant* $j(E_0) = j_0$.
- Then either E_0 or a quadratic twist of E_0 has N points over $\mathbb{F}_\ell$.

Complex multiplication

Let K be a field of characteristic zero, E elliptic curve over K.
Need to define complex multiplication to define the Hilbert class polynomial $H_D(X)$.
Let $\mathrm{End}(E) :=$ endomorphism ring of $E = \{$morphisms $E \to E$ that are group homomorphisms$\}$.

- For most elliptic curves in characteristic zero: $\mathrm{End}(E) = \mathbb{Z}$:
- For all $m \in \mathbb{Z}_{\geq 0}$, we have the "multiplication-by-m" map:

$$[m] : P \mapsto P + \cdots + P \ (m \text{ times})$$

- Can also define "multiplication-by-m" map for negative m.
- For most curves (in characteristic zero): these are all endomorphisms.

Complex multiplication, continued

CM case: $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$.

Definition: E has complex multiplication (CM) by $\mathcal{O}$ if $\mathrm{End}(E)$ is an order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{D})$ with $D < 0$.

Example: $E : y^2 = x^3 - x$ over $\mathbb{C}$ has endomorphism ring $\mathrm{End}(E)$ strictly larger than $\mathbb{Z}$ since it contains a map

$$\phi : (x, y) \mapsto (-x, iy).$$

Easy to check: $\phi \circ \phi$ is $[-1] : P \mapsto -P$. So E has CM by $\mathbb{Z}[i]$.

The Hilbert class polynomial

Now: ready to define j-invariant and Hilbert Class polynomial.

Definition: The j-invariant of $E : y^2 = x^3 + Ax + B$ is

$$j(E) = \frac{256 \cdot 27 \cdot A^3}{4A^3 + 27B^2}$$

We have: $j(E) = j(E') \iff E \cong E'$ over the algebraic closure.

Definition: Let $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$. Let $\mathcal{O}_K$ be the ring of integers. The Hilbert class polynomial $H_D(X)$ of K is the polynomial whose roots are exactly the j-invariants of elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}_K$.

The Hilbert class polynomial, continued

$$H_D(X) = \prod_{E/\mathbb{C} \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K} (X - j(E)).$$

Theorem: The polynomial $H_D(X)$ has integer coefficients.

This implies:
Can reduce H_D modulo ℓ to find curves over $\mathbb{F}_\ell$ whose endomorphism ring is $\mathcal{O}_K$.

Algorithms for Computing Hilbert class polynomials

So to construct elliptic curves with a given number of points, enough to compute the Hilbert class polynomial.

Several methods:

- analytic (Atkin-Morain, 1993)
- p-adic (Couveignes-Henocq, 2002, Bröker, 2007)
- Chinese Remainder Theorem method (Agashe-Lauter-Venkatesan, 2004)
- modified CRT method (Belding-Bröker-Enge-Lauter, 2008)

Running for all of them: exponential in $\log(|D|)$.

This talk: will present the CRT method.

The Chinese Remainder Theorem (CRT) method

CRT algorithm for computing the Hilbert class polynomial of a quadratic imaginary number field K (Agashe-Lauter-Venkatesan, 2004):

1. Compute upper bound B on the coefficients of $H_D(X)$.
2. Compute $H_D(X)$ modulo small primes $p_1, \ldots, p_n$ which split completely in the Hilbert class field of K and such that
$$\prod_i p_i > B.$$
3. Use the Chinese Remainder Theorem to find the coefficients of $H_D(X)$.

Step 2: Computing $H_D(X)$ mod p for small primes p

Can describe what $H_D(X) \pmod{p}$ looks like for certain primes p:

- Let $D < 0$ be the discriminant of the maximal order $\mathcal{O}_K$ of $K := \mathbb{Q}(\sqrt{D})$. Let p be a rational prime such that $4p = t^2 - Du^2$ for some integers u and t.
- Let $\mathrm{Ell}'(D)$ be the set of $\overline{\mathbb{F}}_p$ isomorphism classes of elliptic curves over $\mathbb{F}_p$ with $\mathrm{End}(E) = \mathcal{O}_K$.

Proposition:

$$H_D(X) \pmod{p} = \prod_{[E'] \in \mathrm{Ell}'(D)} (X - j(E')).$$

Step 2: Computing $H_D(X)$ mod p for small primes p, continued

Can compute the set $\mathrm{Ell}'(D)$ when $D =$ discriminant of the maximal order and p is a prime of the form $4p = t^2 - D$:

Proposition: Suppose p is a prime and $t \neq 0$ is an integer such that $4p = t^2 - D$. Let E' be an elliptic curve over $\mathbb{F}_p$. Then $[E'] \in \mathrm{Ell}'(D)$ if and only if $\#E'(\mathbb{F}_p)$ is either $p + 1 - t$ or $p + 1 + t$.

Algorithm for computing all factors of $H_D(X)$ mod p:

1. For each $j \in \mathbb{F}_p$, create an elliptic curve E' over $\mathbb{F}_p$ with $j(E') = j$.
2. If $\#E'(\mathbb{F}_p)$ is either $p + 1 - t$ or $p + 1 + t$, then $H_D(X)$ (mod p) has a factor of $(X - j(E'))$.

Recap of Part 1

Can use elliptic curves for cryptography.

To do this: construct curves with a prescribed number of points.

To construct an elliptic curve E_0 over $\mathbb{F}_\ell$ with N points:

1. Compute the imaginary quadratic number field $K = \mathbb{Q}(\sqrt{D})$ with $\mathrm{End}(E_0) \subseteq K$.
2. Compute Hilbert class polynomial $H_D(X)$ for K by computing $H_D(X) \pmod p$ for many small primes p. (CRT step)
3. Find a root j_0 of $H_D(X)$ modulo ℓ.
4. Construct a curve modulo E_0 over $\mathbb{F}_\ell$ with $j(E_0) = j_0$. This is easy. E_0 or twist of E_0 is the desired curve.

Part 2: Genus 2 curves

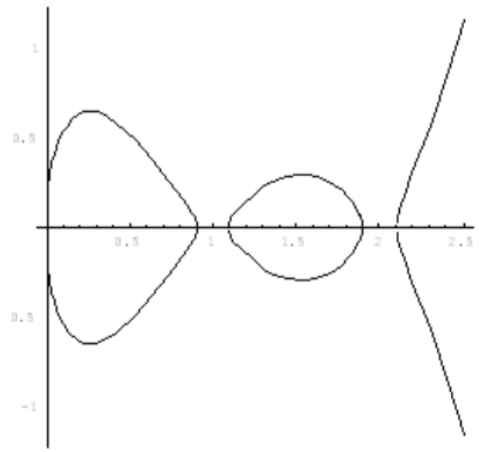
Generalize elliptic curve construction to curves of genus 2.

Advantage for crypto: can work over smaller prime field and get comparable group size.

Definition: Let K be a field of characteristic $\neq 2$. A curve of genus 2 is a smooth projective curve that has an affine model

$$y^2 = f(x), \quad deg(f) = 5 \text{ or } 6,$$

with $f \in K[x]$, f no double roots.



Group law on Jacobians of genus 2 curves

- Group elements: points on the *Jacobian* of the curve.
  The Jacobian of C is the quotient group

$$\mathrm{Jac}(C) = D_0/P.$$

  $D_0 =$ group of degree zero divisors on C
  $P =$ subgroup of principal divisors on C.
- The curve

$$C : y^2 = f(x) \text{ with } \mathrm{degree}(f) = 5$$

  has one point at infinity ∞.
  Elements of Jacobian: represented by divisors

$$D = \sum_{i=1}^{r} P_i - r \cdot \infty \text{ with } P_i \in C \text{ and } r \leq 2.$$

Genus 2 curves with a given number of points on the Jacobian

Let C be a curve of genus 2 over $\mathbb{F}_p$.

Let $P(X)$ be the characteristic polynomial of the Frobenius endomorphism π on $\mathrm{Jac}(C)$.
$P(X)$ is monic of degree 4, has integer coefficients. Roots $a_1, \ldots, a_4$ have absolute value $p^{1/2}$.

$P(X)$ determines the number of points on C and on $\mathrm{Jac}(C)$:

- $\#C(\mathbb{F}_{p^m}) = 1 - \sum_{1=1}^{4} a_i^m + p^m$
- $\#\,\mathrm{Jac}(C)(\mathbb{F}_{p^m}) = \prod_{i=1}^{4}(1 - a_i^m)$
- $\#\,\mathrm{Jac}(C)(\mathbb{F}_p) = \frac{1}{2}\#C(\mathbb{F}_{p^2}) + \frac{1}{2}\#C(\mathbb{F}_p) - p$

Statement of Problem

Algorithm (E-Lauter, 2009): Our algorithm solves the following problem (under certain conditions):

Problem: Given (ℓ, N_1, N_2) with ℓ prime, N_1, N_2 positive integers: construct genus 2 curve C over $\mathbb{F}_\ell$ such that $\#C(\mathbb{F}_\ell) = N_1$ and $\#C(\mathbb{F}_{\ell^2}) = N_2$.

For cryptographic applications: want $\#\operatorname{Jac}(C)(\mathbb{F}_\ell)$ to be prime.

Setup for genus 2 curves

- Want to generalize the algorithm for constructing elliptic curves (i.e. curves of genus 1) to genus 2 setting.
- Need an analogue of the j-invariant and the Hilbert class polynomial.
- Need notion of complex multiplication (CM) for genus 2 curves.

Complex multiplication for genus 2 curves

- Elliptic curves E have CM if $\mathrm{End}(E)$ is an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$.
- A curve C of genus 2 has CM if $\mathrm{End}(\mathrm{Jac}(C))$ is an order in a quartic CM field K, i.e. if $K = K_0(\sqrt{d})$ with K_0 real quadratic and $d \in K_0$ totally negative.
- The genus 2 curves we construct will have CM.

Finding the quartic CM field

Goal: Given (ℓ, N_1, N_2) find a genus 2 curve C defined over $\mathbb{F}_\ell$ such that $\#C(\mathbb{F}_\ell) = N_1$ and $\#C(\mathbb{F}_{\ell^2}) = N_2$.

First Step: Find the quartic CM field K such that $\mathrm{End}(\mathrm{Jac}(C)) \subseteq K$.
To do this: find quartic polynomial satisfied by Frobenius:

- Write

$$N_1 = \ell + 1 - s_1, \quad N_2 = \ell^2 + 1 + 2s_2 - s_1^2.$$

- Solve for s_1, s_2. (Assume $\gcd(s_2, \ell) = 1$.)
- The quartic CM field K is generated over $\mathbb{Q}$ by a root of $X^4 - s_1X^3 + s_2X^2 - \ell s_1 X + \ell^2$.

Elliptic curves versus genus 2 curves

Constructing curves with a given number of points:

Approach for elliptic curve case: To construct the desired curve over $\mathbb{F}_\ell$: Find the (quadratic imaginary) CM field K, then find a root j_0 of the Hilbert class polynomial of K modulo ℓ. Desired curve E_0 over $\mathbb{F}_\ell$ is E_0 with $j(E_0) = j_0$.

Approach for genus 2 case: To construct the desired curve over $\mathbb{F}_\ell$: Find the quartic CM field K. Construct analogue of the Hilbert class polynomial. What is this?

Igusa invariants

For elliptic curves E, E' over $\overline{K}$:
E is isomorphic to $E' \iff j(E) = j(E')$.

Igusa invariants: genus 2 analogue of the j-invariant.
For genus 2 curve $y^2 = f(x)$ over $K = \overline{K}$:

- Igusa defines invariants I_2, I_4, I_6, I_{10}. Gives bijection between isomorphism classes of genus 2 curves over K and points $(I_2 : I_4 : I_6 : I_{10})$ in weighted projective space with $I_{10} \neq 0$.
- From I_2, I_4, I_6, I_{10}: can construct absolute Igusa invariants $i_1 = \frac{I_2^5}{I_{10}}, i_2 = \frac{I_2^3 I_4}{I_{10}}, i_3 = \frac{I_2^2 I_6}{I_{10}}$. They determine the $\overline{K}$-isomorphism classes of curves.

Igusa class polynomials

Let K be a primitive quartic CM field. Let $\mathcal{A}$ be a set of representatives for isomorphism classes Jacobians of genus 2 curves defined over $\mathbb{C}$ with CM by the maximal order $\mathcal{O}_K$. Given $A \in \mathcal{A}$ let $(j_1(A), j_2(a), j_3(A))$ be its triple of absolute Igusa invariants.

The Igusa class polynomials H_1, H_2, H_3 are defined to be

$$H_i(X) = \prod_{A \in \mathcal{A}} (X - j_i(A)) \quad (i = 1, 2, 3).$$

Difficulty: $H_i(X) \in \mathbb{Q}[X]$, not $\mathbb{Z}[X]$. Need bound on denominators (Goren-Lauter, 2011).

Constructing genus 2 curves with a given number of points on its Jacobian

To construct genus 2 curves with a given number of points:

Step 1: Compute the quartic CM field K such that $\mathrm{End}(\mathrm{Jac}(C)) \subseteq K$.

Step 2: Compute the Igusa class polynomials H_1, H_2, H_3 for K.

Outline of CRT algorithm for genus 2 curves

CRT algorithm for computing Igusa class polynomials:

Theorem (E-Lauter): Given a primitive quartic CM field K, the following algorithm finds the Igusa class polynomials of K:

1. Produce a collection S of small primes such that
   - $p \in S$ satisfies certain splitting conditions in K and the reflex field of K.
   - $\prod_{p \in S} p > c$, where c is a constant that depends on the coefficients of the Igusa class polynomials and their denominators.
2. Form the class polynomials H_1, H_2, H_3 modulo p for each $p \in S$.
3. (CRT Step) Form $H_i(X)$ from the collection of H_i modulo p.

Step 2: Computing Igusa class polynomials modulo p

Can describe $H_i(X)$ modulo p for primes that satisfy our splitting conditions:

Proposition (E-Lauter):

$$H_i(X) \pmod{p} = \prod_{C \in T_p} (X - j_i(C)).$$

Here T_p = collection of $\overline{\mathbb{F}}_p$ isomorphism classes of genus 2 curves C over $\mathbb{F}_p$ with $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$.

Use Proposition to compute $H_i(X) \pmod{p}$ for p small:

- Loop through all possible triples of Igusa invariants (j_1, j_2, j_3). For each triple: construct curve C over $\mathbb{F}_p$ with $(j_1, j_2, j_3) = (j_1(C), j_2(C), j_3(C))$ using Mestre's algorithm.
- For each curve C check whether $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

Computing the endomorphism ring of Jac(C)

To compute the Igusa class polynomials: need to be able to test whether $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$.

- First result by E-Lauter (2005): requires computation of action of Frobenius on torsion subgroups.
- Improvement on this by Freeman-Lauter (2007).
- Bisson (2015): General algorithm for computing the endomorphism of the Jacobian of a genus 2 curve: generalizes work of G. Bisson and D. Sutherland for elliptic curves.

Conclusion

- Can use elliptic curves and genus 2 curves for cryptography.

  Advantage over RSA: smaller key size
- To construct genus 2 curves with a given number of points: Compute Igusa class polynomials with a CRT algorithm.
- Open Problems:
  - Make CRT step more efficient by avoiding looping through all triples of Igusa invariants.
  - How to generalize to genus 3?