Genus 2 point counting using isogenies

Jean Kieffer
Supervision: D. Robert, A. Page

Journées Codes et Cryptographie
~~Erdeven, 15–20 March 2020~~ Online, 2–6 November 2020

LFANT team, IMB (Univ. Bordeaux)

The case of elliptic curves

Point counting

Given an elliptic curve $E/\mathbb{F}_p$,

$$E\colon y^2 = x^3 + ax + b, \quad (a, b \in \mathbb{F}_p)$$

compute $\#E(\mathbb{F}_p)$ = group order.

Use in crypto: pick random curves until we find one of prime order.

The case of elliptic curves

Point counting

Given an elliptic curve $E/\mathbb{F}_p$,

$$E\colon y^2 = x^3 + ax + b, \quad (a, b \in \mathbb{F}_p)$$

compute $\#E(\mathbb{F}_p)$ = group order.

Use in crypto: pick random curves until we find one of prime order.

Schoof's algorithm (1985)

For a bunch of small primes ℓ: ℓ-torsion subgroup $E[\ell]$.

$$\mathrm{Frob} \circlearrowleft E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2.$$

$$\#E(\mathbb{F}_p) = p + 1 - \mathrm{Tr}_{E[\ell]}(\mathrm{Frob}) \mod \ell.$$

Then, Chinese remainders. Polynomial time in $\log p$, but slow.

The SEA algorithm (Schoof–Elkies–Atkin)

Replace $E[\ell]$ by a subgroup $K \simeq \mathbb{Z}/\ell\mathbb{Z}$:

$$K = \text{kernel of an } \ell\text{-isogeny } \phi\colon E \to E' \text{ defined over } \mathbb{F}_p.$$

Elkies's method to compute $\#E(\mathbb{F}_p)$ mod ℓ:

1. See if such an ℓ-isogeny ϕ exists. If not, pick another ℓ.
2. Compute the kernel K.
3. Compute Frobenius eigenvalue λ, then $\mathrm{Tr} = \lambda + p/\lambda \mod \ell$.

Crucial improvement over Schoof's algorithm: $\#K = \ell$, not ℓ^2.

Computing isogenies from modular equations

Detecting an ℓ-isogeny

with the help of the ℓ-th classical modular polynomial $\Phi_\ell(X, Y)$:

$$\phi \text{ exists} \iff \Phi_\ell(j(E), Y) \text{ has a root over } \mathbb{F}_p.$$

Computing the kernel

- Construct $E'/\mathbb{F}_p$ such that $\Phi_\ell(j(E), j(E')) = 0$.
- Several algorithms to compute an ℓ-isogeny $\phi \colon E \to E'$ are known (Elkies 90's, Bostan et al. 2006, ...)

Plan

1. The genus 2 setting
2. The isogeny algorithm
3. Application to point counting

The genus 2 setting

Genus 2 curves and their Jacobians

Let $\mathcal{C}$ be a smooth genus 2 curve over $\mathbb{F}_p$,

$$\mathcal{C}\colon v^2 = f(u), \quad \deg(f) \in \{5, 6\}.$$

- Group law on the Jacobian $\mathrm{Jac}(\mathcal{C})$.
  $\mathrm{Jac}(\mathcal{C})$ has dimension 2: abelian surface.
- Generically,

  point on $\mathrm{Jac}(\mathcal{C})$ = unordered pair of points on $\mathcal{C}$.

Jacobians of genus 2 curves are (generically) characterized up to isomorphism by three Igusa invariants: j_1, j_2, j_3.

Modular equations in genus 2

ℓ-isogenies

- $\mathrm{Jac}(\mathcal{C})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^4$ with a Weil pairing.
- An ℓ-isogeny $\phi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}')$ is such that

$$\ker\phi \subset \mathrm{Jac}(\mathcal{C})[\ell], \qquad \ker\phi \simeq (\mathbb{Z}/\ell\mathbb{Z})^2 \text{ and isotropic.}$$

ℓ-isogenies

- $\mathrm{Jac}(\mathcal{C})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^4$ with a Weil pairing.
- An ℓ-isogeny $\phi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}')$ is such that

$$\ker\phi \subset \mathrm{Jac}(\mathcal{C})[\ell], \qquad \ker\phi \simeq (\mathbb{Z}/\ell\mathbb{Z})^2 \text{ and isotropic.}$$

Siegel modular equations

Three equations Ψ_1, Ψ_2, Ψ_3 that vanish on Igusa invariants of ℓ-isogenous Jacobians:

$$\begin{cases} \Psi_1(j_1, j_2, j_3, j_1') = 0 \\ j_2' = \Psi_2(j_1, j_2, j_3, j_1') \\ j_3' = \Psi_3(j_1, j_2, j_3, j_1'). \end{cases}$$

The isogeny algorithm

Computing isogenies from modular equations

Let $\mathcal{C}$, $\mathcal{C}'$ be genus 2 curves s.t. $\mathrm{Jac}(\mathcal{C})$, $\mathrm{Jac}(\mathcal{C}')$ are ℓ-isogenous.

Problem

Compute an ℓ-isogeny $\phi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}')$.

Representing ϕ

$$\mathrm{Jac}(\mathcal{C}) \xrightarrow{\ \phi\ } \mathrm{Jac}(\mathcal{C}')$$

Computing isogenies from modular equations

Let $\mathcal{C}$, $\mathcal{C}'$ be genus 2 curves s.t. $\mathrm{Jac}(\mathcal{C})$, $\mathrm{Jac}(\mathcal{C}')$ are ℓ-isogenous.

Problem

Compute an ℓ-isogeny $\phi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}')$.

Representing ϕ

$$\mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C}) \xrightarrow{\phi} \mathrm{Jac}(\mathcal{C}')$$

- Choice of base point P defines an embedding $\mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C})$

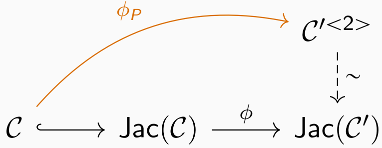
Computing isogenies from modular equations

Let $\mathcal{C}$, $\mathcal{C}'$ be genus 2 curves s.t. $\mathrm{Jac}(\mathcal{C})$, $\mathrm{Jac}(\mathcal{C}')$ are ℓ-isogenous.

Problem

Compute an ℓ-isogeny $\phi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}')$.

Representing ϕ



- Choice of base point P defines an embedding $\mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C})$
- Describe image by a pair of points on $\mathcal{C}'$:

$$\phi_P(u, v) = \langle (x_1, y_1), (x_2, y_2) \rangle$$

- Compute $x_1 + x_2 = S(u, v)$, etc.

Differential forms

Equation of $\mathcal{C} \to$ basis of differential forms on $\mathcal{C}$:

$$\omega = \left(\frac{u\,du}{v}, \frac{du}{v} \right).$$

ω is also a basis of differential forms on $\mathrm{Jac}(\mathcal{C})$.

The normalization matrix

$\mathcal{C}, \mathcal{C}'$ define bases ω, ω'.

$$m \in \mathrm{GL}_2(\mathbb{F}_p) : \text{ matrix of } \phi^* \text{ in the bases } \omega', \omega.$$

The isogeny algorithm

1. Compute the normalization matrix m:

   Use derivatives of modular equations, and computations with Siegel modular forms.

2. Solve a differential system to compute ϕ_P:

$$\begin{cases} \dfrac{x_1\,dx_1}{y_1} + \dfrac{x_2\,dx_2}{y_2} = (m_{1,1}u + m_{2,1})\dfrac{du}{v} \\ \dfrac{dx_1}{y_1} + \dfrac{dx_2}{y_2} = (m_{1,2}u + m_{2,2})\dfrac{du}{v} \\ y_1^2 = f_{\mathcal{C}'}(x_1) \\ y_2^2 = f_{\mathcal{C}'}(x_2) \end{cases}$$

   Solve locally around P using power series in a uniformizer z, then rational reconstruction.

Application to point counting

Smaller subgroups

Point counting

Given $\mathcal{C}$, compute $\#\,\mathrm{Jac}(\mathcal{C})(\mathbb{F}_p)$.

As before: study subgroups of $\mathrm{Jac}(\mathcal{C})[\ell]$ with Frobenius action.

Isogenies yield smaller subgroups

$$\text{Full torsion } (\mathbb{Z}/\ell\mathbb{Z})^4 \rightsquigarrow \text{Kernel of isogeny } (\mathbb{Z}/\ell\mathbb{Z})^2$$

The real multiplication case

$\mathbb{Z}_K \hookrightarrow \mathrm{End}(\mathrm{Jac}(\mathcal{C}))$, $\quad K$ fixed real quadratic field.

$$\text{Kernel of endomorphism } (\mathbb{Z}/\ell\mathbb{Z})^2 \rightsquigarrow \text{Kernel of isogeny } \mathbb{Z}/\ell\mathbb{Z}$$

Cost comparison

Cost comparison for a curve over $\mathbb{F}_p$, using asymptotically fast polynomial multiplication.

Balance smaller subgroups with the cost of evaluating modular equations.

	Classical Schoof	**Isogenies (SEA)**
Elliptic curves	$\widetilde{O}(\log(p)^5)$	$\widetilde{O}(\log(p)^4)$
Genus 2	$\widetilde{O}(\log(p)^8)$	$\widetilde{O}(\log(p)^8)$
Genus 2, small height	$\widetilde{O}(\log(p)^8)$	$\widetilde{O}(\log(p)^7)$
Genus 2, with RM	$\widetilde{O}(\log(p)^5)$	$\widetilde{O}(\log(p)^4)$

Implementation

Implementation is on the way.

- Evaluating modular equations in the RM case with $K = \mathbb{Q}(\sqrt{5})$ is quite fast (a few minutes) when ℓ is in the hundreds.
- Can we beat a point-counting record?

Questions?

Thank you!

Evaluating modular equations

Let's consider elliptic curves. We want to evaluate

$$\Phi_\ell(j(E), X) \in \mathbb{F}_p[X].$$

Using complex approximations:

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$.
2. Find a floating-point $\tau \in \mathbb{H}_1$ such that $j(\tau) = \widetilde{j}$.
3. Evaluate j at every $\frac{\gamma\tau}{\ell}$, where γ runs through $\Gamma_0(\ell)\backslash \mathrm{SL}_2(\mathbb{Z})$.
4. Compute
$$\Phi_\ell(\widetilde{j}, X) = \prod_\gamma \left(X - j\left(\frac{\gamma\tau}{\ell}\right)\right).$$
5. Recognize integer coefficients from approximations.
6. Reduce to $\mathbb{F}_p$.