Generating random supersingular Elliptic Curves using modular polynomials

Simon Pohmann
Supervisor: Cristophe Petit

June 7, 2022

Elliptic Curves

Definition

An *Elliptic Curve* is a projective variety with a defining equation of the form

$$y^2z = x^3 + Axz^2 + Bz^3$$

- Affine points of E are $(x, y) \in \bar{k}^2$ such that $y^2 = x^3 + Ax + B$

Elliptic Curves

Definition

An *Elliptic Curve* is a projective variety with a defining equation of the form

$$y^2z = x^3 + Axz^2 + Bz^3$$

- Affine points of E are $(x, y) \in \bar{k}^2$ such that $y^2 = x^3 + Ax + B$
- One point "at infinity"

Elliptic Curves

Definition

An *Elliptic Curve* is a projective variety with a defining equation of the form

$$y^2z = x^3 + Axz^2 + Bz^3$$

- Affine points of E are $(x, y) \in \bar{k}^2$ such that $y^2 = x^3 + Ax + B$
- One point "at infinity"
- E defined over field k if $A, B \in k$

Elliptic Curves are groups

Proposition

Let E be an Elliptic Curve over k. Then there is $+_E : E \times E \to E$ such that E becomes a group.
Further, $+_E$ is (locally) given by polynomials.

- E is an *algebraic group*

Elliptic Curves are groups

Proposition

Let E be an Elliptic Curve over k. Then there is $+_E : E \times E \to E$ such that E becomes a group.
Further, $+_E$ is (locally) given by polynomials.

- E is an *algebraic group*
- For $x_1 \neq x_2$, define $(x_1, y_1) +_E (x_2, y_2)$ to be

$$\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,\ (2x_1 + x_2)\frac{y_2 - y_1}{x_2 - x_1} - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 - y_1\right)$$

Isogenies

Definition

An algebraic map (i.e. morphism) between Elliptic Curves $E \to E'$ is called isogeny, if it maps $\infty \mapsto \infty$.

- "algebraic map" = "locally given by polynomials"

Isogenies

Definition

An algebraic map (i.e. morphism) between Elliptic Curves $E \to E'$ is called isogeny, if it maps $\infty \mapsto \infty$.

- "algebraic map" = "locally given by polynomials"
- isogenies are automatically group homomorphisms

Isogenies

Definition

An algebraic map (i.e. morphism) between Elliptic Curves $E \to E'$ is called isogeny, if it maps $\infty \mapsto \infty$.

- "algebraic map" = "locally given by polynomials"
- isogenies are automatically group homomorphisms
- important subclass: *separable* isogenies

Isogenies

Definition

An algebraic map (i.e. morphism) between Elliptic Curves $E \to E'$ is called isogeny, if it maps $\infty \mapsto \infty$.

- "algebraic map" $=$ "locally given by polynomials"
- isogenies are automatically group homomorphisms
- important subclass: *separable* isogenies
- 1-1 correspondence

$$\begin{aligned} \text{separable isogenies } E \to E' \quad &\leftrightarrow \quad \text{subgroups } G \leq E \\ \phi \quad &\mapsto \quad \ker(\phi) \end{aligned}$$

Isogenies

Definition

An algebraic map (i.e. morphism) between Elliptic Curves $E \to E'$ is called isogeny, if it maps $\infty \mapsto \infty$.

- "algebraic map" = "locally given by polynomials"
- isogenies are automatically group homomorphisms
- important subclass: *separable* isogenies
- 1-1 correspondence

$$\begin{array}{rcl} \text{separable isogenies } E \to E' & \leftrightarrow & \text{subgroups } G \leq E \\ \phi & \mapsto & \ker(\phi) \end{array}$$

- degree of separable isogeny is $\# \ker(\phi)$

Isogenies

Definition

An algebraic map (i.e. morphism) between Elliptic Curves $E \to E'$ is called isogeny, if it maps $\infty \mapsto \infty$.

- "algebraic map" $=$ "locally given by polynomials"
- isogenies are automatically group homomorphisms
- important subclass: *separable* isogenies
- 1-1 correspondence

$$\begin{aligned} \text{separable isogenies } E \to E' \;&\leftrightarrow\; \text{subgroups } G \leq E \\ \phi \;&\mapsto\; \ker(\phi) \end{aligned}$$

- degree of separable isogeny is $\# \ker(\phi)$
- l-isogeny $:=$ degree l isogeny

Isogenies (continued)

Definition

An algebraic map (i.e. morphism) between Elliptic Curves $E \to E'$ is called isogeny, if it maps $\mathcal{O} \mapsto \mathcal{O}$.

- Group law given by polynomials

$$\Rightarrow \text{have isogeny} \quad [m] : E \to E, \quad P \mapsto \underbrace{P + ... + P}_{m \text{ times}}$$

Isogenies (continued)

Definition

An algebraic map (i.e. morphism) between Elliptic Curves $E \to E'$ is called isogeny, if it maps $\mathcal{O} \mapsto \mathcal{O}$.

- Group law given by polynomials

$$\Rightarrow \text{have isogeny} \quad [m] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{m \text{ times}}$$

- If E defined over $\mathbb{F}_q$

$$\Rightarrow \text{have isogeny} \quad \pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$$

Supersingular and ordinary curves

The endomorphisms (isogenies $E \to E$) of E form a ring $\mathrm{End}(E)$.

- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ as $[m]$ is isogeny

Supersingular and ordinary curves

The endomorphisms (isogenies $E \to E$) of E form a ring $\mathrm{End}(E)$.

- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ as $[m]$ is isogeny

Proposition

If $k = \mathbb{F}_q$ is a finite field, then one of the following holds

- $\mathrm{End}(E)$ *is an order in a quadratic imaginary number field*
- $\mathrm{End}(E)$ *is an order in a quaternion algebra*

Supersingular and ordinary curves

The endomorphisms (isogenies $E \to E$) of E form a ring $\mathrm{End}(E)$.

- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ as $[m]$ is isogeny

Proposition

If $k = \mathbb{F}_q$ is a finite field, then one of the following holds

- $\mathrm{End}(E)$ *is an order in a quadratic imaginary number field*
- $\mathrm{End}(E)$ *is an order in a quaternion algebra*

Definition

In the first case, E is called *ordinary*, otherwise *supersingular*.

Isogeny graphs

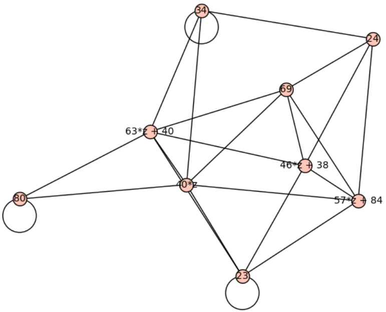
Elliptic Curves up to isomorphism are classified by *j-invariant* $j(E)$

- l-isogeny graph: $V = \{j(E) \mid E \text{ defined over } \mathbb{F}_q\}$
  $E = \{(j(E), j(E') \mid \exists\ l\text{-isogeny } E \to E')\}$

Isogeny graphs

Elliptic Curves up to isomorphism are classified by *j-invariant* $j(E)$

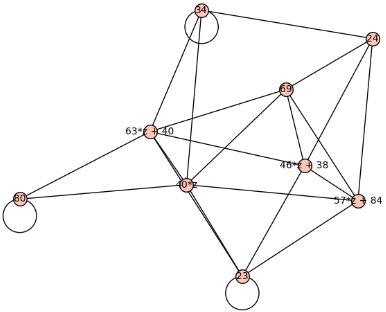
- l-isogeny graph: $V = \{j(E) \mid E \text{ defined over } \mathbb{F}_q\}$
  $E = \{(j(E), j(E') \mid \exists\ l\text{-isogeny } E \to E')\}$
- The supersingular l-isogeny graph is an expander



Isogeny graphs

Elliptic Curves up to isomorphism are classified by *j-invariant* $j(E)$

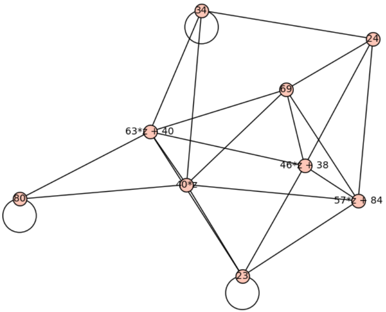
- l-isogeny graph: $V = \{j(E) \mid E \text{ defined over } \mathbb{F}_q\}$
  $E = \{(j(E), j(E')) \mid \exists\ l\text{-isogeny } E \to E')\}$
- The supersingular l-isogeny graph is an expander
  - Useful for cryptography

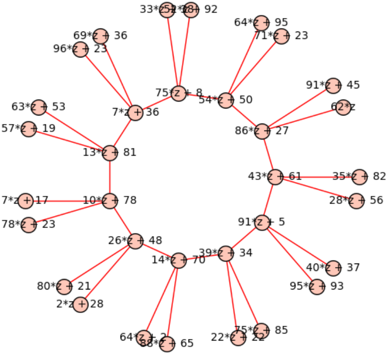


Isogeny graphs

Elliptic Curves up to isomorphism are classified by *j-invariant* $j(E)$

- l-isogeny graph: $V = \{j(E) \mid E \text{ defined over } \mathbb{F}_q\}$
  $E = \{(j(E), j(E')) \mid \exists\ l\text{-isogeny } E \to E')\}$
- The supersingular l-isogeny graph is an expander
  - Useful for cryptography
- Ordinary l-isogeny graphs are "volcanoes"





Generating supersingular curves

- Classical approach: Random walk in isogeny graph

Generating supersingular curves

- Classical approach: Random walk in isogeny graph

Question

Is there a method that does not reveal a path to a fixed curve?

Generating supersingular curves

- Classical approach: Random walk in isogeny graph

Question

Is there a method that does not reveal a path to a fixed curve?

- Experiments have shown correlation between supersingularity and having (multiple) l-isogenies $E \to E^{(p)}$, for fixed l.
  - First explored in [Boo+22], with limited success

Generating supersingular curves

- Classical approach: Random walk in isogeny graph

Question

Is there a method that does not reveal a path to a fixed curve?

- Experiments have shown correlation between supersingularity and having (multiple) l-isogenies $E \to E^{(p)}$, for fixed l.
  - First explored in [Boo+22], with limited success

Question

How many ordinary resp. supersingular curves with l-isogeny $E \to E^{(p)}$ exist?

Modular Polynomials

Proposition

There is a polynomial $\Phi_l(x, y) \in \mathbb{Z}[x, y]$ *such that* $\Phi_l(j(E), j(E')) = 0$ *if and only if there is an* l*-isogeny* $E \to E'$.

Modular Polynomials

Proposition

There is a polynomial $\Phi_l(x, y) \in \mathbb{Z}[x, y]$ *such that* $\Phi_l(j(E), j(E')) = 0$ *if and only if there is an* l*-isogeny* $E \to E'$*.*

- Finding a curve with l-isogeny $E \to E^{(p)}$ is as easy/as hard as finding a root of $\Phi_l(x, x^p)$

Modular Polynomials

Proposition

There is a polynomial $\Phi_l(x,y) \in \mathbb{Z}[x,y]$ *such that* $\Phi_l(j(E), j(E')) = 0$ *if and only if there is an l-isogeny* $E \to E'$*.*

- Finding a curve with l-isogeny $E \to E^{(p)}$ is as easy/as hard as finding a root of $\Phi_l(x, x^p)$
- Finding a curve with an l_1-and an l_2 isogeny $E \to E^{(p)}$ corresponds to finding a root of $\gcd(\Phi_{l_1}(x,x^p), \Phi_{l_2}(x,x^p))$

Modular Polynomials

Proposition

There is a polynomial $\Phi_l(x, y) \in \mathbb{Z}[x, y]$ *such that* $\Phi_l(j(E), j(E')) = 0$ *if and only if there is an* l*-isogeny* $E \to E'$*.*

- Finding a curve with l-isogeny $E \to E^{(p)}$ is as easy/as hard as finding a root of $\Phi_l(x, x^p)$
- Finding a curve with an l_1-and an l_2 isogeny $E \to E^{(p)}$ corresponds to finding a root of $\gcd(\Phi_{l_1}(x, x^p), \Phi_{l_2}(x, x^p))$

Modular Polynomials

Proposition

There is a polynomial $\Phi_l(x, y) \in \mathbb{Z}[x, y]$ such that $\Phi_l(j(E), j(E')) = 0$ if and only if there is an l-isogeny $E \to E'$.

- Finding a curve with l-isogeny $E \to E^{(p)}$ is as easy/as hard as finding a root of $\Phi_l(x, x^p)$
- Finding a curve with an l_1-and an l_2 isogeny $E \to E^{(p)}$ corresponds to finding a root of $\gcd(\Phi_{l_1}(x, x^p), \Phi_{l_2}(x, x^p))$

Question

Is there a way to find a root of $\gcd(\Phi_{l_1}(x, x^p), \Phi_{l_2}(x, x^p))$ for exponentially large l_1, l_2 (and of course p)?

Thank you for your attention!

Jeremy Booher et al. *Failing to hash into supersingular isogeny graphs*. Cryptology ePrint Archive, Report 2022/518. https://ia.cr/2022/518. 2022.