Computing Isogenies. (Joint work with Kristin Lauter & René Schoof)

~~Problem:~~ Motivation: Let $E/\mathbb{F}_p$ be an elliptic curve.

Suppose $P \in E(\mathbb{F}_q)$ and m is an integer

we can compute $[m]P$ in time $O(\log m \log^2 q)$

by repeated doubling $[m] = 2^k + a_1 2^{k-1} + \dots + a_k$

$P, 2P, 2^2 P, \dots, 2^k P.$

Time complexity can be written as $O(\log(\underbrace{\deg [m]}_{m^2}) \log^2 q)$.

Question: For which maps $\psi: E \to E'$ can we evaluate $\psi(P)$ in time $O(\log \deg \psi \log^2 q)$?

$(P \in E(\mathbb{F}_q))$ or $\log^{O(1)} \deg \psi \log^2 q$.

Currently $O(\deg^{1+\varepsilon} \psi \log^2 q)$

$(\log \deg \psi)(\log q)^{O(1)}$

Maps between elliptic curves:

Let $E_1/\mathbb{F}_p$ k be ~~two~~ elliptic curves

& $E_2/\mathbb{F}_p$ k

A homomorphism $f: E_1 \to E_2$ is a morphism of algebraic curves (locally given by polynomials project. or rationals functions).

that is also a group homomorphism.

An <u>isogeny</u> is a non-zero homomorphism.

A homomorphism $f: E \to E$ is called an endomorphism.

Facts: An isogeny is automatically surjective with finite kernel.

Let $E \xrightarrow{\varphi} E'$ be an isogeny of elliptic curves over k.

Then
$$\begin{array}{c} k(E) \\ \uparrow \\ k(E') \end{array}$$
the degree of this extension is called $\deg \varphi$.

If this extension is separable then $\# \ker \varphi = \deg \varphi$.
$[m]$ has degree m^2. and separable if $m \perp \operatorname{char} k$.
If k is the finite field
π is not separable (purely inseparable) $(x,y) \mapsto (x^p, y^p)$

If
$$\begin{tikzcd} E \arrow[r, "\varphi"] & E' \arrow[l, bend left, "\hat{\varphi}"] \end{tikzcd}$$
$\hat{\varphi} \circ \varphi = [\deg \varphi]_E$

$\varphi \circ \hat{\varphi} = [\deg \varphi]_{E'}$

$$\begin{tikzcd} & E' \arrow[d, "\cong"] \\ E \arrow[ur, "\varphi_1"] \arrow[r, "\varphi_2"'] & E' \end{tikzcd}$$

$[m]$ is self dual $[m] \circ [m] = [m^2]$

$\hat{\varphi}$ is called the dual isogeny.

An isogeny is determined upto isomorphism by its kernel.

We will be interested in prime degree isogenies of degree $\ell \neq p = \operatorname{char} k$.
so will be separable.

$E \xrightarrow{\varphi} E'$ φ is degree ℓ

then $\# \ker \varphi = \ell$. $\Rightarrow$ $\ker \varphi \subseteq E[\ell]$

But ~~ker~~ $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ $(\ell \neq p)$.

$\langle Q \rangle$, $\langle P + iQ \rangle$ $0 \leq i \leq \ell - 1$.

There are $\ell+1$ subgroups of order ℓ in $E[\ell]$,

so upto isomorphism there are $\ell+1$ isogenies of degree ℓ from E.

Maps that we are interested in computing are isogenies of prime degree.

We say a homormorphism f is defined over k if the equations defining f have coefficients in k. $[m]$ defined over $\mathbb{F}_p$

Write End (E) for the endomorphism ring of E (absolute) or $End_{\bar{k}}(E)$

$\varphi : E \to E'/k$, k finite field, $\varphi \circ \pi_E = \pi_{E'} \circ \varphi$.

Note: If $\varphi : E \to E'$ is an isogeny defined over $\mathbb{F}_{p^r}$ then we will need $\Omega(r \log p)$ bit operations to evaluate it!

If E is an ordinary elliptic curve then $End(E)$ is an order, $\mathcal{O}$, in a ~~quadratic~~ imaginary quadratic field.

The isomorphisms of E are the units in $\mathcal{O}$.

Let $K = End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. $\qquad \mathcal{O}_K$ = maximal order

$End(E) = \mathcal{O}$

Then $\mathbb{Z}[\pi] \subseteq \mathcal{O}$ where π is the Frobenius map on E $(x, y) \mapsto (x^p, y^p)$.

$\pi^2 - t\pi + q = 0$

Note: If $\alpha \in \mathbb{Z}[\pi]$ $\quad \alpha = a + b\pi$ (separable iff $p \nmid a$)

$$\deg[\alpha] = \mathrm{Norm}_{K/\mathbb{Q}}\, \alpha.$$

$$= a^2 + ab(\pi + \bar{\pi}) + b^2 \pi\bar{\pi}$$

π satisfies $\pi^2 - t\pi + q = 0$

$$= a^2 + abt + b^2 p \geq a^2 + b^2 p - 2ab\sqrt{p}$$

$$\frac{\deg[\alpha]}{a} = a + bt + \frac{b^2}{a} p$$

Also $a + b\pi$ can be computed in $\log^3 q \deg[\alpha]$ time.

Vélu's formulae: 1971. (for any field k)

Let $E/\mathbb{F}_p$ be an elliptic curve

$G \subseteq E(\overline{\mathbb{F}}_p)$.

Velu gives the equations for the isogeny $\varphi: E \to E/G$

Let $k(E) = k(x,y)$

$$x_G(P) = x(P) + \sum_{Q \in G - \{0\}} \left(x(P+Q) - x(Q) \right)$$

$$y_G(P) = y(P) + \sum_{Q \in G - \{0\}} \left(y(P+Q) - y(Q) \right)$$

these are in $k(E)$ and ~~invariant~~ leave G invariant.
maps $P \in G$ to $\mathcal{O}$.

claim: x_G & y_G generate $k(E/G)$ $\quad \varphi: P \mapsto (x_G(P), y_G(P))$

From this he finds the equations for φ.
Let $|G| = l$ an odd prime
Suppose $E: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

$Q \in E - \{0\}$

$$g^x(Q) = 3x^2 + 2a_2x + a_4 - a_1y$$
$$g^y(Q) = -2y - a_1x - a_3.$$
$$t(Q) = 2g^x(Q) - a_1g^y(Q)$$
$$u(Q) = (g^y(Q))^2$$

$$t = \sum_{Q \in G - \{0\}} t(Q) \qquad w = \sum_{Q \in (G - \{0\})} \left(u(Q) + x(Q)t(Q) \right)$$

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

$A_1 = a \qquad A_2 = a_2 \qquad A_3 = a_3$

$A_4 = a_1 - 5t \qquad A_6 = a_6 - b_2t - 7w.$

Using Vélu requires $O(\ |G|\ (\log^2 q + \log^2 q'))$

to evaluate $\psi(P)$ where $P \in E(\mathbb{F}_q)$

and $G \subseteq E(\mathbb{F}_{q'})$.

If $\deg \psi = \ell$ q' could be q^{ℓ^2} $O(\ell^3 \log^2 q)$

Lots of improvements Morain, Couveignes
Bostan, Morain, Salvy, ~~Schost~~ Schost
Elkies

$O(\ \ell \log \ell \log\log \ell\ )$ ops $/ \mathbb{F}_q$.

Waterhouse - Abelian varieties over finite fields 1969. P. 1.

Let $E/\mathbb{F}_p$ be an ordinary curve.

$\phi : E \to E'$ an isogeny defined over $\mathbb{F}_p$. (commutes with Frobenius).

$\pi_E : E \to E$ $\qquad \pi_{E'} : E' \to E'$ the p^{th} power Frobenius

$\phi \circ (\pi_E) = \pi_{E'} \phi$. $\quad \mathcal{O}_K$ (ϕ surjective)

we got $\quad \mathrm{End}(E) \qquad \mathrm{End}(E')$

$$\mathrm{End}(E) \supseteq \mathbb{Z}[\pi] \subseteq \mathrm{End}(E')$$

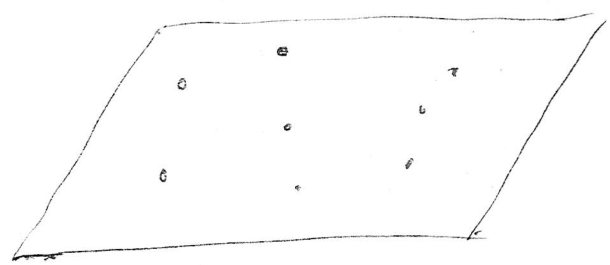
Let $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ an imaginary quadratic field.

If E' is isogenous to E then its endomorphism ring $\mathcal{O}'$

$$\mathcal{O}_K \supseteq \mathcal{O}' \supseteq \mathbb{Z}[\pi]$$

among these there are some curves with the same endomorphism ring call this set $Ell(\mathcal{O})$

Let I be an ideal in $\mathcal{O}$.



$\mathrm{End}(E) = \mathcal{O}$

Take $G = \bigcap_{\alpha \in I} \ker \alpha$

G is a finite group $\quad \# G = Nm\, I$.

$\mathrm{End}\, E/G = \mathrm{End}(E) = \mathcal{O}$. $\qquad I = \{ \rho \mid \rho G = 0 \}$
I is a kernel ideal.

$\alpha \in \mathcal{O}$ then for every $\tau \in I$ $\quad \alpha\tau \in I$.

$P \in \alpha(G) \Rightarrow \quad \alpha \tau(P) = 0 \quad \forall \tau \in I$

$\Rightarrow \gamma(P) = 0 \quad \forall \gamma \in I$

$\Rightarrow P \in G$. $\qquad$ So G is fixed by α.

G is fixed by $\mathcal{O}$ so $\mathcal{O} \subseteq \mathrm{End}(E/G)$ equality follows from $I = \{ \rho \mid \rho G = 0 \}$.

What we have so far:

let $E/\mathbb{F}_p$: $\mathrm{End}(E) = \mathcal{O}$.

$I \subseteq \mathcal{O}$ an ideal then $E/_{\ker I}$ has same endomorphism ring.

Proposition:
~~Suppose~~ $A/_{G_1} \cong A/_{G_2}$ iff $\exists\ \rho \in \mathrm{End}(A)$

$0 \neq N \in \mathbb{Z}$: $\rho^{-1} G_1 = N^{-1} G_2$.

Corollary: Let $I_1 = \beta I_2$ $\quad \beta \in K$.

$\Rightarrow \quad I_1 = \dfrac{\rho}{n} I_2$ $\quad$ for $\rho \in$ ~~End~~ $\mathcal{O}$ and n an integer.

$\Rightarrow \quad n I_1 = \rho I_2$.

$G_1 = \ker I_1, \qquad G_2 = \ker I_2$.

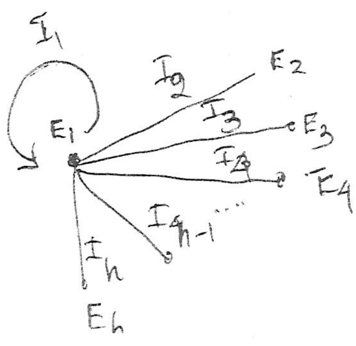
$$\rho^{-1} G_2 = \ker \rho I_2$$
$$\|$$
$$n^{-1} G_1 = \ker n I_1$$

$\Rightarrow$ If $I_1 \sim I_2$ in $Cl(\mathcal{O})$ then $E/_{\ker I_1} \cong E/_{\ker I_2}$.

Theorem: (Waterhouse) Let $Ell(\mathcal{O})$ be the set of (non-supersingular) elliptic curves over $\mathbb{F}_p$ with endomorphism ring $\mathcal{O}$. Then $Cl(\mathcal{O})$ acts on $Ell(\mathcal{O})$ with the action being free with one orbit.

Waterhouse)

free: $g x \neq h x \quad \forall x,\ h \neq g$.



$\Rightarrow \#Ell(\mathcal{O}) = \#Cl(\mathcal{O})$.

One orbit: $Ell(\mathcal{O}) = \{ E \cdot Cl(\mathcal{O}) \}$

m is conductor of $\mathbb{Z}[\pi]$

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)}{[\mathcal{O}_K^* : \mathcal{O}^*]}\, m \prod_{\substack{\ell \mid m \\ \text{prime}}} \left(1 - \left(\frac{D_K}{\ell}\right)\frac{1}{\ell}\right).$$

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

$\mathcal{O} \subseteq K$ endomorphism ring

$\ell \nmid [\mathcal{O}_K : \mathcal{O}] \times \mathrm{disc}(K)$

ℓ splits in $\mathcal{O}_K$.

$Cl(\mathcal{O})$ the class group of $\mathcal{O}$

$I_1, I_2, \ldots, I_h$ the ideal generators for $Cl(\mathcal{O})$.

☆ Decompose $(\ell) = \mathfrak{l}_1 \mathfrak{l}_2$ ~~on $Cl(\mathcal{O})$~~ in $\mathcal{O}$.
be the prime decomposition in $\mathcal{O}$.
$\mathcal{O}/(\ell) \cong \mathcal{O}_K/(\ell)$.

Decompose $\mathfrak{l}_1 = (\alpha)\, \cancel{I_1^{e_1}}\, I_2^{e_2} \cdots I_h^{e_h}$
~~Let~~ Let $\mathfrak{l}_1 = (\alpha) I_1$
α a principal fractional ideal.
α a principal fractional ideal.

Suppose $\mathfrak{l}_1 = (\alpha) I_1$
and ψ is the isogeny with $\ker \mathfrak{l}_1 = \ker \psi$
Let ψ_1 = isogeny such that $\ker \psi_1 = \ker I_1$

$$\alpha = \frac{\beta}{n} \qquad \beta \in \mathrm{End}$$

$$\beta = \frac{a + b\pi}{n}$$

$$\psi(P) = \psi_1(\underbrace{(a+b\pi)}_{\beta}\, Q)$$

where Q is a point such that $nQ = P$.

$$\beta = a + b\sqrt{D}$$

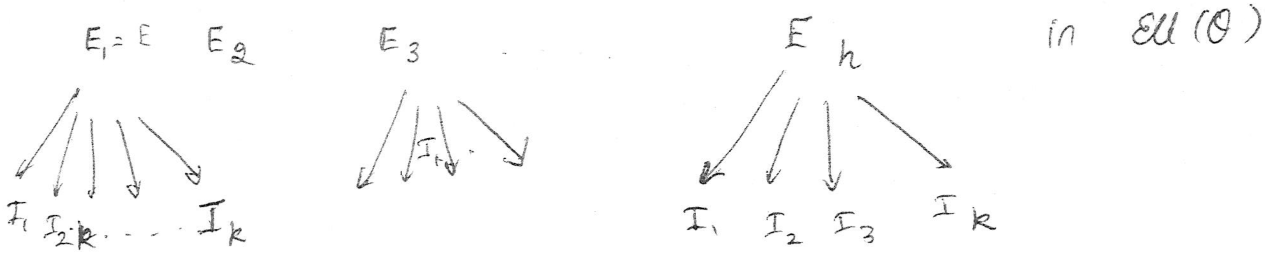
How do we find Q : $nQ = P$?

Suppose $\gcd(n, \#E(\mathbb{F}_p)) = 1$

then $Q = mP$ where $mn \equiv 1 \mod \#E(\mathbb{F}_p)$.

β can be written as $a + b\pi$ with $a, b \in \mathbb{Z}$

so for points P on $E(\mathbb{F}_p)$ this simply becomes multiplication by some scalar.



Compute Q and then compose the isogenies according to the factorization that we got to compute $\psi(P)$.

$$E \xrightarrow{I_1} E_2 \xrightarrow{I_3} E_4$$

How do we get the isogeny corresponding to I_1 ?

Let $I_1 = (a + b\pi_D, \; c + d\pi_D)$

$(a + b\pi_D)(P) = 0$ $\qquad y^2 = f(x)$

$aP = (-b\pi_D)(P)$

$P = (x, y)$

$$nP = \left(\frac{\phi_n(x,y)}{\psi_n(x,y)^2}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3} \right)$$

$$= \frac{\phi_{b\sqrt{D}}(x^P, y)}{\psi_{b\sqrt{D}}(x,y)^2}$$

$$\frac{\phi_a(x,y)}{\psi_a(x,y)^2} = \frac{\phi_b(x^P, y^P)}{\psi_b(x^P, y^P)^2}$$

for odd n these can be calculated as polynomials in x and the curve coefficients a_i.

As the kernel is stable under the map $[-1]$, we can get a polynomial $\psi_{a+b\pi} \in k[x]$ that defines the x-coordinates of the kernel of the endomorphism $a+b\pi$.

Similarly, we have another polynomial $\psi_{c+d\pi} \in k[x]$ whose kernel is that of the endomorphism $c+d\pi$.

$$\ker \alpha_1 = \gcd(\psi_{a+b\pi}, \psi_{c+d\pi}).$$

Using this polynomial one can write down the equation of this isogeny,

Method runs in polynomial time if $cl(\mathcal{O})$ is small eg. for curves produced by CM method! disc $\mathcal{O}$ is small

Q: There are $l+1$ isogenies of degree l, what about the other isogenies?

$$E \xrightarrow{\varphi} E'$$

φ constructed as we did has the property that $\mathrm{End}(E) = \mathrm{End}(E')$

and that φ is defined over $\mathbb{F}_p$.

Proposition: If $E \xrightarrow{\varphi} E'$ and φ an isogeny of degree l, then either $\mathcal{O} = \mathcal{O}'$ or

$[\mathcal{O} : \mathcal{O}'] = l$ ~~or~~

$[\mathcal{O}' : \mathcal{O}] = l$.

Furthermore, $\mathcal{O} = \mathcal{O}'$ iff $\ker \varphi = \ker I$ for some ideal I in $\mathcal{O}$.

Thus the other isogenies (of which there are $\ell-1$) change the endomorphism ring.

A note on the field of definition (Atkin).

$\varphi: E \to E'$ is defined over $\mathbb{F}_{p^r}$ if

$$\pi^r(\ker\varphi) = \ker\varphi \quad \text{(but not necessarily fixed pointwise).}$$

$\Rightarrow$ $\ker\varphi$ is a 1-dimensional eigenspace for π^r.

(In fact, the modular polynomial $\phi_\ell(x,y)$ satisfies

$\phi_\ell(j, T) = 0$ has a root in $\mathbb{F}_{p^r}$ iff
π^r has a 1-dimensional eigenspace.)

All the isogenies $E \xrightarrow{\varphi} E'$ are defined over $\mathbb{F}_{p^r}$ iff
π^r operates as a scalar matrix on $E[\ell]$.

Consider $\pi: E[\ell] \to E[\ell]$

π operates by some matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_\ell)$

$$\begin{pmatrix} \alpha & \underset{\text{non-zero}}{*} \\ 0 & \alpha \end{pmatrix} \quad \Rightarrow \quad \ell \mid t^2 - 4p$$

we have one isogeny defined over $\mathbb{F}_p$
and the rest defined over an extension $\mathbb{F}_{p^\ell}$.

$$\pi \sim \begin{pmatrix} \alpha & 0 \\ * & \beta \end{pmatrix} \qquad \left(\frac{t^2 - 4p}{\ell}\right) = +1 \quad \text{split case.}$$

Two isogenies are defined over $\mathbb{F}_p$ (as we saw)

the other isogenies defined over $\mathbb{F}_{p^r}$ where

$$r = \mathrm{lcm}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta)).$$

$$r \mid \ell - 1.$$

π acts irreducibly on $E[\ell]$ $\qquad \left(\frac{t^2-4p}{\ell}\right) = -1$ Inert case.

π acts as mult by $\alpha \in \mathbb{F}_{\ell^2}^*$ on $(\mathbb{Z}/\ell\mathbb{Z})^2$.

then all isogenies are defined over an extension $\mathbb{F}_{p^r}$ where $r \mid (\ell+1)$.