Computing the trace of a supersingular endomorphism

or, Beyond the SEA (algorithm)

Travis Morrison

Virginia Tech

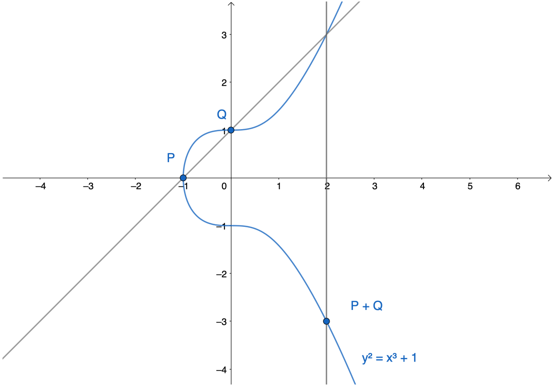
joint work with: Lorenz Panny, Jana Sotáková, Michael Wills

Elliptic curves

- Let k be a field. An *elliptic curve over k* is given by an equation

$$E : y^2 = x^3 + Ax + B,$$

  where $A, B \in k$ and $4A^3 + 27B^2 \neq 0$.
- The rational points of E, denoted $E(k)$, form a group under the group law
  'three colinear points sum to zero, and zero is the point at infinity.'



Isogenies and endomorphisms of elliptic curves

Let E, E' be elliptic curves over k.

Definition

An *isogeny* $\phi\colon E \to E'$ is a rational map that induces a group homomorphism $E(\overline{k}) \to E'(\overline{k})$. An *endomorphism* of E is an isogeny $\phi : E \to E$.

- If n is an integer, then the multiplication-by-n map

$$[n] : P \mapsto nP$$

  is an endomorphism of E
- If $k = \mathbb{F}_q$, then the *Frobenius endomorphism* of E is an endomorphism:

$$\begin{aligned} \pi_E\colon E &\to E \\ (x, y) &\mapsto (x^q, y^q). \end{aligned}$$

Degrees, duals, and traces

Definition

- The **degree** of an isogeny $\phi \colon E \to E'$ is its degree as a rational map. When ϕ is separable, $\deg \phi = \# \ker \phi$.
- Every isogeny $\phi \colon E \to E'$ has a unique **dual isogeny** $\widehat{\phi} \colon E' \to E$ satisfying $\widehat{\phi} \circ \phi = [\deg \phi]$.
- The dual map is an involution on $\mathrm{End}(E)$: $\widehat{\alpha + \beta} = \widehat{\alpha} + \widehat{\beta}$, $\widehat{\alpha\beta} = \widehat{\beta}\widehat{\alpha}$.
- The **trace** of an endomorphism α is the integer t such that

  $$\alpha + \widehat{\alpha} = [t].$$

  Every endomorphism satisfies its **characteristic polynomial**

  $$x^2 - (\mathrm{tr}\, \alpha)x + \deg \alpha.$$

- E is **supersingular** if $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra.

A cheatsheet

	Endomorphisms	Imaginary quadratic integers
Notation	α	$a + b\sqrt{-D}$
Involution	The dual map	complex conjugation
Norm	$\deg \alpha = \widehat{\alpha} \circ \alpha$	$\lvert a + b\sqrt{-D}\rvert^2 = a^2 + Db^2$
Trace	$\operatorname{tr} \alpha = \alpha + \widehat{\alpha}$	$2a$

Examples, again

- Let $[n]\colon E \to E$ be the multiplication-by-n map. We have

$$\deg[n] = n^2, \quad \operatorname{tr}[n] = 2n.$$

Examples, again

- Let $[n]\colon E \to E$ be the multiplication-by-n map. We have

$$\deg[n] = n^2, \quad \operatorname{tr}[n] = 2n.$$

- Let π_E be the Frobenius endomorphism of $E/\mathbb{F}_q$. Then

$$\deg \pi_E = q, \quad \operatorname{tr} \pi_E = q + 1 - \#E(\mathbb{F}_q)$$

Examples, again

- Let $[n]\colon E \to E$ be the multiplication-by-n map. We have
$$\deg[n] = n^2, \quad \operatorname{tr}[n] = 2n.$$
- Let π_E be the Frobenius endomorphism of $E/\mathbb{F}_q$. Then
$$\deg \pi_E = q, \quad \operatorname{tr} \pi_E = q + 1 - \#E(\mathbb{F}_q)$$
- Hasse bound: $|\operatorname{tr} \pi_E| \leq 2\sqrt{q}$

Examples, again

- Let $[n]: E \to E$ be the multiplication-by-n map. We have

$$\deg[n] = n^2, \quad \operatorname{tr}[n] = 2n.$$

- Let π_E be the Frobenius endomorphism of $E/\mathbb{F}_q$. Then

$$\deg \pi_E = q, \quad \operatorname{tr} \pi_E = q + 1 - \#E(\mathbb{F}_q)$$

- Hasse bound: $|\operatorname{tr} \pi_E| \le 2\sqrt{q}$
- More generally, if $\alpha \in \operatorname{End}(E)$, then

$$\operatorname{disc} \alpha = (\operatorname{tr} \alpha)^2 - 4 \deg \alpha \le 0 \implies |\operatorname{tr} \alpha| \le 2\sqrt{\deg \alpha}.$$

Computing the trace of an endomorphism

Problem: computing traces of endomorphisms

Given an elliptic curve $E/\mathbb{F}_q$ and $\alpha \in \mathrm{End}(E)$, compute $\mathrm{Tr}\,\alpha := \alpha + \widehat{\alpha} \in \mathbb{Z}$.

Computing the trace of an endomorphism

Problem: computing traces of endomorphisms

Given an elliptic curve $E/\mathbb{F}_q$ and $\alpha \in \mathrm{End}(E)$, compute $\mathrm{Tr}\,\alpha := \alpha + \widehat{\alpha} \in \mathbb{Z}$.

Why? Ordinary case

Point counting! Also, $\mathrm{tr}\,\pi_E$ reveals the structure of $\mathbb{Z}[\pi_E]$ as an algebra.

Computing the trace of an endomorphism

Problem: computing traces of endomorphisms

Given an elliptic curve $E/\mathbb{F}_q$ and $\alpha \in \mathrm{End}(E)$, compute $\mathrm{Tr}\,\alpha := \alpha + \widehat{\alpha} \in \mathbb{Z}$.

Why? Ordinary case

Point counting! Also, $\mathrm{tr}\,\pi_E$ reveals the structure of $\mathbb{Z}[\pi_E]$ as an algebra.

Why? Supersingular case

Four endomorphisms $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ span $\mathrm{End}(E) \iff \det(\mathrm{tr}(\alpha_i \widehat{\alpha_j}))_{i,j} = p^2$.

Moreover, computing traces yields a multiplication table for the basis $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

Schoof's algorithm

If we know

$$t_\ell := \operatorname{tr}\alpha \pmod{\ell}$$

for primes ℓ such that $\prod_\ell \ell > 4\sqrt{\deg\alpha}$ then we can recover $\operatorname{tr}\alpha$ with the CRT.

Schoof's algorithm

If we know

$$t_\ell := \operatorname{tr}\alpha \pmod{\ell}$$

for primes ℓ such that $\prod_\ell \ell > 4\sqrt{\deg\alpha}$ then we can recover $\operatorname{tr}\alpha$ with the CRT.

Algorithm 2: Schoof's algorithm

Input: Ordinary $E/\mathbb{F}_q$
Output: $\operatorname{tr}(\pi_E)$
Set $\ell = 2$ and $M = 1$;
while $M \leq 4\sqrt{q}$ **do**
  Compute $t_\ell = \operatorname{tr}\pi_E \bmod \ell$;
  Update $M = M \cdot \ell$;
  Update ℓ with the next prime after ℓ;
Solve $t \equiv t_\ell \pmod{\ell}$ for $t \in [-2\sqrt{q}, 2\sqrt{q}]$ with CRT;
return t

Computing $t_\ell = \operatorname{tr}\alpha \bmod \ell$

Suppose $(\ell, q) = 1$. An endomorphism $\alpha \in \operatorname{End}(E)$ acts on $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ as a "matrix"

$$\alpha_\ell := \alpha\big|_{E[\ell]} \in \operatorname{End}(E[\ell]) \cong M_2(\mathbb{Z}/\ell\mathbb{Z})$$

Computing $t_\ell = \operatorname{tr}\alpha \bmod \ell$

Suppose $(\ell, q) = 1$. An endomorphism $\alpha \in \mathrm{End}(E)$ acts on $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ as a "matrix"

$$\alpha_\ell := \alpha\big|_{E[\ell]} \in \mathrm{End}(E[\ell]) \cong M_2(\mathbb{Z}/\ell\mathbb{Z})$$

Schoof's method for computing t_ℓ

Compute t_ℓ by computing the characteristic polynomial of α_ℓ. We have

$$\operatorname{tr}\alpha \equiv \operatorname{Tr}(\alpha_\ell) \pmod{\ell}.$$

Rather than working with points in $E[\ell]$: find $0 \leq c < \ell$ such that

$$\alpha_\ell^2 + [\deg\alpha]_\ell = c\alpha_\ell$$

by computing coordinate functions modulo the **division polynomial** ψ_ℓ, the monic polynomial vanishing precisely $x(P)$ for $P \neq 0 \in E[\ell]$

Computing $\operatorname{tr} \pi_E$

Let $E/\mathbb{F}_p$ be given by $y^2 = f(x)$ and $\alpha = \pi_E$ and $n = \lceil \log p \rceil$.

The cost of computing t_ℓ is dominated by the cost of computing

$$\pi_\ell = (x^p \bmod \psi_\ell(x), (f^{(p-1)/2} \bmod \psi_\ell(x))y)$$

Since $\deg \psi_\ell = (\ell^2 - 1)/2$, can compute $\operatorname{tr} \pi_E \pmod{\ell}$ in $O(n^4 \log n)$ bit operations (fast euclidean division, Kronecker substitution, fast euclidean algorithm, and $\mathrm{M}(n) = O(n \log n)$ (Harvey–van der Hoeven)).

By the Prime Number Theorem: require t_ℓ for $O(n/\log n)$ primes ℓ, resulting in a $O(n^5)$ algorithm for computing $\operatorname{tr} \pi_E$.

Rational isogenies

Let $E : y^2 = f(x)$ be defined over $\mathbb{F}_q$. Every separable isogeny $\phi\colon E \to E'$ has a **standard form**[1]

$$\phi(x,y) = \left(\frac{u(x)}{v(x)}, c\left(\frac{u(x)}{v(x)}\right)' y\right), \quad \text{where } v(x) = \prod_{0 \neq P \in \ker\phi} (x - x(P)).$$

We have $\deg u = \deg v + 1 = \deg \psi$.

ϕ is $\mathbb{F}_q$-rational $\iff$ $c \in \mathbb{F}_q$ and $u/v \in \mathbb{F}_q(x)$ $\iff$ $c \in \mathbb{F}_q$, $\ker\phi$ is $\mathrm{Gal}(\overline{\mathbb{F}_q})$-stable.

Write $v = \gcd(f,v)g^2$. Then $h(x) := \gcd(f,v)g$ is the **kernel polynomial** of ϕ. When ϕ is normalized (i.e. $c = 1$), ϕ is defined over $\mathbb{F}_q$ if and only if $h(x) \in \mathbb{F}_q[x]$.

[1] Bostan–Morain–Salvy–Schost, 2008

Elkies' method for computing $t_\ell = \operatorname{tr} \pi_E \bmod \ell$

For 50% of primes ℓ (asymptotically), ℓ is an **Elkies' primes** for E, meaning E admits a $\mathbb{F}_q$-rational ℓ-isogeny ϕ. Note ϕ is rational $\iff$ π_E fixes $\ker\phi \subset E[\ell]$. In this case,

$$\pi_E\big|_{\ker\phi} \in \operatorname{End}(\ker\phi) \cong \mathbb{Z}/\ell\mathbb{Z}$$

Elkies' method for computing $t_\ell = \operatorname{tr} \pi_E \bmod \ell$

For 50% of primes ℓ (asymptotically), ℓ is an **Elkies' primes** for E, meaning E admits a $\mathbb{F}_q$-rational ℓ-isogeny ϕ. Note ϕ is rational $\iff$ π_E fixes $\ker\phi \subset E[\ell]$. In this case,

$$\pi_E\big|_{\ker\phi} \in \operatorname{End}(\ker\phi) \cong \mathbb{Z}/\ell\mathbb{Z}$$

By working modulo the **kernel polynomial** $h(x)$ of ϕ, find $0 \le c < \ell$ such that

$$\alpha^2\big|_{\ker\phi} + [\deg\alpha]\big|_{\ker\phi} = c(\alpha\big|_{\ker\phi})$$

Then $t_\ell = c$. This gives a speedup of a factor of $\ell = O(\log p)$ in computing t_ℓ, because

$$\deg\psi_\ell = (\ell^2-1)/2, \quad \deg h(x) = (\ell-1)/2.$$

Assuming heuristics "beyond" GRH, the SEA algorithm computes $\operatorname{tr}\pi_E$ in $O(n^4(\log n)^2)$ bit operations ($n = \log p$).

Representing endomorphisms

Now assume $\alpha \in \mathrm{End}(E)$ is represented by a sequence of L many $\mathbb{F}_q$-rational isogenies ϕ_i of degree at most d, each ϕ_i in standard form:

$$\alpha = \phi_L \circ \cdots \circ \phi_1.$$

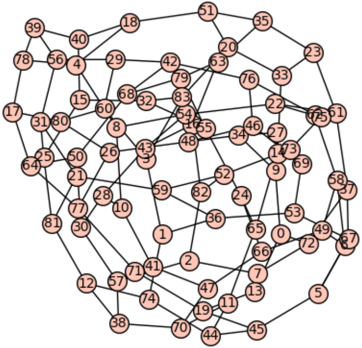


Figure: $G(313, 2)$, The 2-isogeny graph in characteristic 313

Schoof's algorithm for supersingular endomorphisms

Assume $\alpha = \phi_L \circ \cdots \circ \phi_1$ is an endomorphism of $E/\mathbb{F}_q$, each $\phi_i = (u_i/v_i, ys_i/t_i)$ in standard form, ℓ an odd prime. Compute $t_\ell := \operatorname{tr} \alpha \bmod \ell$ by finding $0 \leq c < \ell$ such that

$$\alpha_\ell^2 + [\deg \alpha]_\ell = c\alpha_\ell.$$

To compute $\alpha_\ell = \alpha\big|_{E[\ell]}$: let $(a(x), b(x)y) = (x, y)$ and then for $i = 1, \ldots, L$ update

$$(a, by) = \left(\frac{u_i(a)}{v_i(a)}, \frac{s_i(a)}{t_i(a)} by\right)$$

where arithmetic takes place in $\mathbb{F}_q[x]/(\psi_\ell(x))$.

Letting $n = \lceil \log q \rceil$ and assuming $d = O(1)$ and $L = O(n)$, we have a $O(n^4 \log n)$ algorithm for computing t_ℓ and a $O(n^5)$ algorithm for $\operatorname{tr} \alpha$.

Every prime is an Elkies prime for a supersingular elliptic curve

Proposition

Suppose $E/\mathbb{F}_q$ is supersingular, where $q = p^a$ is a prime power, and let $\phi\colon E \to E'$ be an isogeny. If $j(E) \neq 0, 1728$,

$$\ker\phi \text{ is defined over } \begin{cases} \mathbb{F}_q & : a \text{ is even} \\ \mathbb{F}_{q^2} & : a \text{ is odd.} \end{cases}$$

Every prime is an Elkies prime for a supersingular elliptic curve

Proposition

Suppose $E/\mathbb{F}_q$ is supersingular, where $q = p^a$ is a prime power, and let $\phi\colon E \to E'$ be an isogeny. If $j(E) \neq 0, 1728$,

$$\ker\phi \text{ is defined over } \begin{cases} \mathbb{F}_q & : a \text{ is even} \\ \mathbb{F}_{q^2} & : a \text{ is odd.} \end{cases}$$

Proof: Suppose $q = p^{2a}$. Then (Waterhouse 69) $\operatorname{tr}\pi_E = \pm 2p^a$ so $\pi_E = [\pm p^a]$, so

$$\operatorname{End}_{\overline{\mathbb{F}_q}}(E) = \operatorname{End}_{\mathbb{F}_q}(E).$$

If $\phi\colon E \to E'$ is an isogeny, then $I = \operatorname{Hom}(E', E)\phi$ is a left ideal of $\operatorname{End}(E)$, and

$$\ker\phi = \bigcap_{\alpha\in I} \ker\alpha.$$

All $\ker\alpha$ are $\mathbb{F}_q$-rational, so $\ker\phi$ is $\mathbb{F}_q$-rational.

The SEA algorithm for supersingular endomorphisms

Suppose $E/\mathbb{F}_q$ is supersingular. Then $j(E) \in \mathbb{F}_{p^2}$.

- Assume E itself is defined over $\mathbb{F}_{p^2}$, and $j(E) \neq 0, 1728$.
- In this case, $\pi_E = [\pm p]$.

The SEA algorithm for supersingular endomorphisms

Suppose $E/\mathbb{F}_q$ is supersingular. Then $j(E) \in \mathbb{F}_{p^2}$.

- Assume E itself is defined over $\mathbb{F}_{p^2}$, and $j(E) \neq 0, 1728$.
- In this case, $\pi_E = [\pm p]$.

Then $E/\mathbb{F}_{p^2}$ has **all** of its ℓ-isogenies defined over $\mathbb{F}_{p^2}$.

- Every prime is an Elkies prime for supersingular E!
- But $\alpha \in \mathrm{End}(E)$ need not fix $\ker \phi$
- Compute $\mathrm{tr}\,\alpha \bmod \ell$ by finding c such that the characteristic equation

$$\alpha^2\big|_{\ker \phi} + [\deg \alpha]\big|_{\ker \phi} = c(\alpha\big|_{\ker \phi})$$

holds in $\mathrm{Hom}(\ker \phi, E[\ell])$

The SEA algorithm for supersingular endomorphisms

Assume

- $\alpha = \phi_L \circ \cdots \circ \phi_1$ is an endomorphism of $E/\mathbb{F}_{p^2}$,
- each $\phi_i = (u_i/v_i, ys_i/t_i)$ in standard form,
- ℓ an odd prime, and $h(x) \in \mathbb{F}_q[x]$ is the kernel polynomial of an ℓ-isogeny ϕ.

Goal: Compute $0 \leq c < \ell$ such that

$$\alpha^2\big|_{\ker\phi} + [\deg \alpha]\big|_{\ker\phi} = c(\alpha\big|_{\ker\phi}).$$

The SEA algorithm for supersingular endomorphisms

Assume

- $\alpha = \phi_L \circ \cdots \circ \phi_1$ is an endomorphism of $E/\mathbb{F}_{p^2}$,
- each $\phi_i = (u_i/v_i, ys_i/t_i)$ in standard form,
- ℓ an odd prime, and $h(x) \in \mathbb{F}_q[x]$ is the kernel polynomial of an ℓ-isogeny ϕ.

Goal: Compute $0 \leq c < \ell$ such that

$$\alpha^2\big|_{\ker\phi} + [\deg\alpha]\big|_{\ker\phi} = c(\alpha\big|_{\ker\phi}).$$

To compute $\alpha\big|_{\ker\phi}$: let $(a(x), b(x)y) = (x, y)$ and then for $i = 1, \ldots, L$ update

$$(a, by) = \left(\frac{u_i(a)}{v_i(a)}, \frac{s_i(a)}{t_i(a)}by\right)$$

where arithmetic takes place in $\mathbb{F}_q[x]/(h(x))$.

Theorem (M.–Panny–Sotáková–Wills)

Let $\alpha = \phi_L \circ \cdots \circ \phi_1$ be an endomorphism of a supersingular elliptic curve E defined over $\mathbb{F}_q$, let $n = \lceil \log p \rceil$, and let $\ell = O(n)$ be an odd prime. Let $d = \max\{\deg \phi_i\}$. Then $t_\ell := \operatorname{tr} \alpha \pmod{\ell}$ can be computed in an expected $O(n^3(\log n)^3 + dLn^2 \log n)$ bit operations.

The time complexity simplifies to $O(n^3(\log n)^3)$ when $d = O(1)$ and $L = O(n)$.

- Work projectively, so we only need $O(1)$ inversions in $\mathbb{F}_q[x]/(h(x))$
- Complexity estimate uses fast euclidean division, Kronecker substitution, $\mathrm{M}(n) = O(n \log n)$ (HvdH2019).
- Where's GRH?? Kunzweiler-Robert (ANTS 2024) give an *unconditional* algorithm to compute $\Phi_\ell(X, Y)$ in time $O(\ell^3(\log \ell)^3)$!

Theorem (M.–Panny–Sotáková–Wills)

Let $\alpha = \phi_L \circ \cdots \circ \phi_1$ *be a separable endomorphism of a supersingular elliptic curve* E *defined over* $\mathbb{F}_q$ *with* $j(E) \neq 0, 1728$. *Let* $n = \lceil \log q \rceil$. *Assume that* $L \log d = O(n)$. *Then* $\operatorname{tr} \alpha$ *can be computed with* $O(n^4 (\log n)^2 + dLn^3)$ *bit operations. When* $d = O(1)$ *and* $L = O(n)$, *the complexity is* $O(n^4 (\log n)^2)$.

Beyond the SEA algorithm: computing t_ℓ for $\ell | \#E(\mathbb{F}_{p^2})$

Since we assume $E/\mathbb{F}_{p^2}$ is supersingular and $j(E) \neq 0, 1728$, we know $\#E(\mathbb{F}_{p^2}) = (p \pm 1)^2$. To compute $t_\ell = \operatorname{tr} \alpha \bmod \ell$ for $\ell | \#E(\mathbb{F}_{p^2})$:

1. find $P \neq 0 \in E[\ell](\mathbb{F}_{p^2})$
2. Compute $(\alpha + \widehat{\alpha})(P)$
3. solve a small discrete log: t_ℓ is the solution to

$$cP = (\alpha + \widehat{\alpha})(P).$$

Beyond the SEA algorithm: computing t_p

Let ω_E be an invariant differential for E. Then $\alpha^*\omega_E = c_\alpha \omega_E$ for some $c_\alpha \in \mathbb{F}_{p^2}$, and the map

$$\begin{aligned} \mathrm{End}(E) &\to \mathbb{F}_{p^2} \\ \alpha &\mapsto c_\alpha \end{aligned}$$

is a homomorphism of rings, and (when E is supersingular)

$$\operatorname{tr} \alpha \equiv \operatorname{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p} c_\alpha \pmod{p}.$$

Beyond the SEA algorithm: computing t_p

Let ω_E be an invariant differential for E. Then $\alpha^*\omega_E = c_\alpha \omega_E$ for some $c_\alpha \in \mathbb{F}_{p^2}$, and the map

$$\begin{aligned} \mathrm{End}(E) &\to \mathbb{F}_{p^2} \\ \alpha &\mapsto c_\alpha \end{aligned}$$

is a homomorphism of rings, and (when E is supersingular)

$$\operatorname{tr} \alpha \equiv \operatorname{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p} c_\alpha \pmod{p}.$$

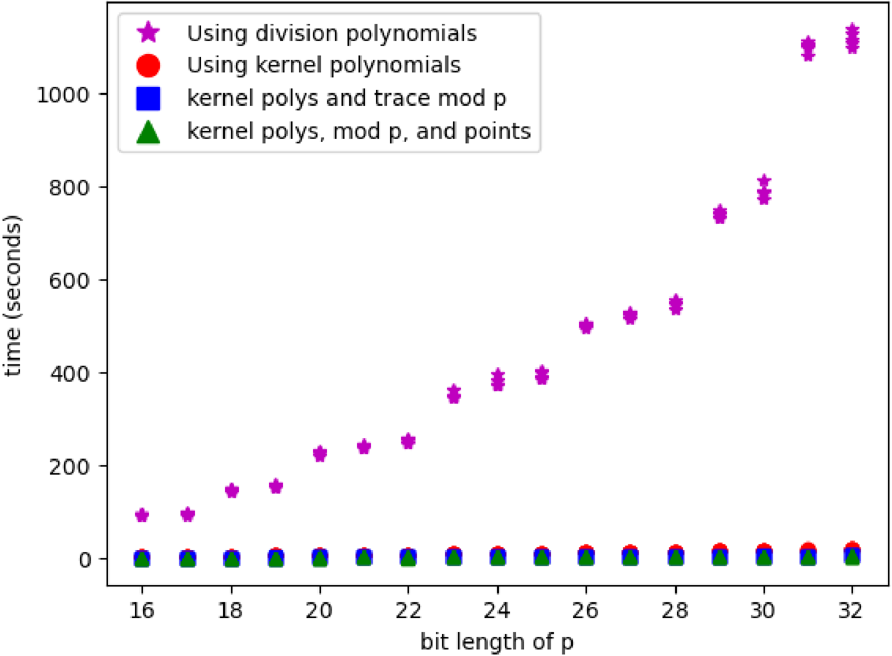
We can "read off" c_α from α: for separable α, we have

$$\alpha(x, y) = \left(\frac{N(x)}{D(x)}, c_\alpha \cdot \left(\frac{N(x)}{D(x)} \right)' y \right)$$

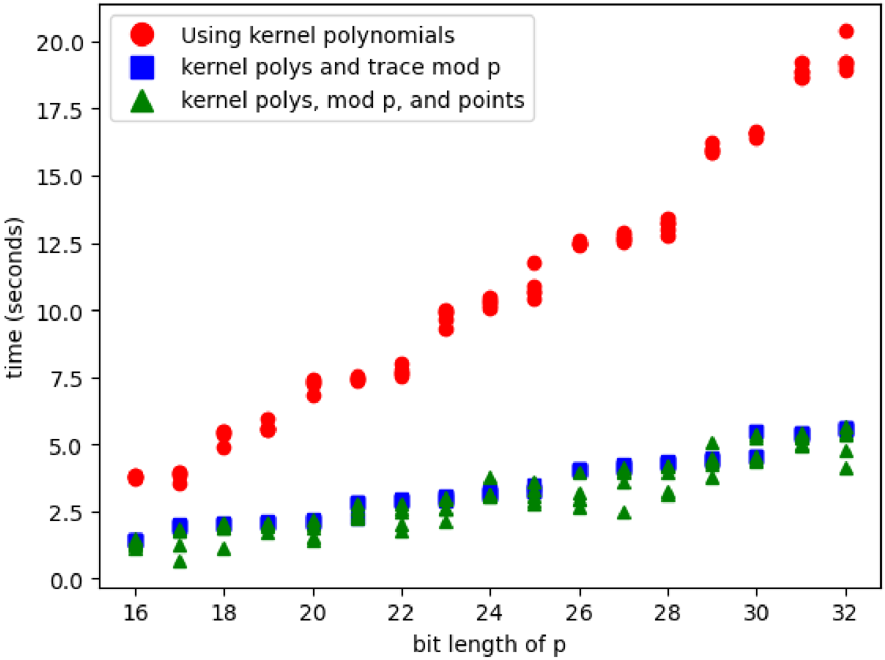
Timings

Implemented in sagemath. To demonstrate the asymptotic speedups offered:

1. For each $b \in [16, \ldots, 32]$, repeat 5 times:
   1. Compute random b-bit prime p, pseudorandom supersingular $E/\mathbb{F}_{p^2}$, and endomorphism $\alpha \in \mathrm{End}(E)$ of degree $\approx p^4$
   2. Compute $\mathrm{tr}\,\alpha$ using Schoof (i.e. get t_ℓ with division polynomials), SEA (i.e get t_ℓ with kernel polynomials), SEA + "mod p", SEA + "mod p" + "points"



Using division polynomials
Using kernel polynomials
kernel polys and trace mod p
kernel polys, mod p, and points
1000
800
600
400
200
0
time (seconds)
16
18
20
22
24
26
28
30
32
bit length of p


Using kernel polynomials
kernel polys and trace mod p
kernel polys, mod p, and points
time (seconds)
bit length of p
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0
16
18
20
22
24
26
28
30
32

Thank you! Questions?