Computing the trace of a supersingular endomorphism

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

Virginia Tech

René 25
University of French Polynesia

Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p

By René Schoof

Abstract. In this paper we present a deterministic algorithm to compute the number of $\mathbf{F}_q$-points of an elliptic curve that is defined over a finite field $\mathbf{F}_q$ and which is given by a Weierstrass equation. The algorithm takes $O(\log^9 q)$ elementary operations. As an application we give an algorithm to compute square roots mod p. For fixed $x \in \mathbf{Z}$, it takes $O(\log^9 p)$ elementary operations to compute $\sqrt{x} \bmod p$.

Counting points on elliptic curves over finite fields

par René SCHOOF

ABSTRACT. —We describe three algorithms to count the number of points on an elliptic curve over a finite field. The first one is very practical when the finite field is not too large; it is based on Shanks's baby-step-giant-step strategy. The second algorithm is very efficient when the endomorphism ring of the curve is known. It exploits the natural lattice structure of this ring. The third algorithm is based on calculations with the torsion points of the elliptic curve [18]. This deterministic polynomial time algorithm was impractical in its original form. We discuss several practical improvements by Atkin and Elkies.

Point counting on elliptic curves

Given $a, b \in \mathbb{F}_p$, compute the number of points on the elliptic curve given by

$$E\colon y^2 = x^3 + ax + b$$

Point counting on elliptic curves

Given $a, b \in \mathbb{F}_p$, compute the number of points on the elliptic curve given by

$$E\colon y^2 = x^3 + ax + b$$

$$\#E(\mathbb{F}_p) = 1 + \#\{(x_0, y_0) \in \mathbb{F}_p^2 : y_0^2 = x_0^3 + ax_0 + b\}.$$

Testing all pairs (x_0, y_0) takes $\widetilde{O}(p^2) = \widetilde{O}(2^{2n})$ time, where $n = \log p$ is the size of the input.

Lang-Trotter: use the equation

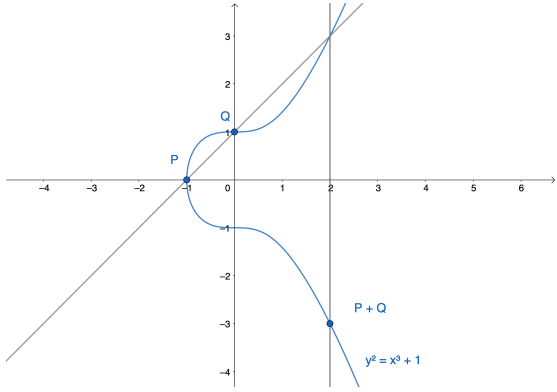
E is given by $y^2 = x^3 + ax + b$. Then

$$\#E(\mathbb{F}_p) = 1 + \sum_{x_0 \in \mathbb{F}_p} \left(1 + \left(\frac{x_0^3 + ax_0 + b}{p}\right)\right).$$

This takes $\widetilde{O}(p) = \widetilde{O}(2^n)$ time.

Mestre: use the group structure

Mestre's algorithm takes $\widetilde{O}(p^{1/4}) = \widetilde{O}(2^{n/4})$ time.



Schoof: use the Frobenius endomorphism

The **Frobenius endomorphism** of E is

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

The fixed points of π are precisely $E(\mathbb{F}_p)$, so

$$\#E(\mathbb{F}_p) = \#\ker(1-\pi) = \deg(1-\pi) = (1-\pi)(1-\widehat{\pi}) = 1 - \operatorname{tr}\pi + p.$$

Compute $\#E(\mathbb{F}_p)$ by computing $\operatorname{tr}\pi$, the **trace of Frobenius**.

Schoof's algorithm

By the Hasse bound $|\operatorname{tr}\pi| \leq 2\sqrt{p}$, if we know

$$t_\ell \coloneqq \operatorname{tr}\pi \pmod{\ell}$$

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

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

Suppose $(\ell, p) = 1$. An endomorphism $\pi \in \mathsf{End}(E)$ acts on $E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ as a "matrix"

$$\pi_\ell \coloneqq \pi\big|_{E[\ell]} \in \mathsf{End}(E[\ell]) \simeq M_2(\mathbb{Z}/\ell\mathbb{Z})$$

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

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

$$\pi_\ell := \pi\big|_{E[\ell]} \in \mathrm{End}(E[\ell]) \simeq M_2(\mathbb{Z}/\ell\mathbb{Z})$$

Schoof's method for computing t_ℓ

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

$$\operatorname{tr}\pi \equiv \mathrm{Tr}\,(\pi_\ell) \pmod{\ell}.$$

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

$$\pi_\ell^2 + [p]_\ell = c\pi_\ell$$

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 $\operatorname{tr} \pi$

Theorem (Schoof)

There is a deterministic polynomial time algorithm to compute $\#E(\mathbb{F}_p)$.

Let $E/\mathbb{F}_p$ be given by $y^2 = f(x)$ 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 $\operatorname{tr} \pi \pmod{\ell}$ 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 $\operatorname{tr} \pi$.

```
sage: E = EllipticCurve(GF(2^255-19), [0,486662,0,1,0])
sage: %time E.cardinality()
CPU times: user 1.56 s, sys: 11.6 ms, total: 1.57 s
Wall time: 1.59 s
57896044618658097711785492504343953926856930875039260848015607506283634007912
sage:
```

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

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

$$\pi\big|_{\ker\phi} \in \mathsf{End}(\ker\phi) \simeq \mathbb{Z}/\ell\mathbb{Z}$$

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

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

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

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

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

Then $t_\ell = c$.

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

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

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

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

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

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 a heuristic, the SEA algorithm computes $\operatorname{tr}\pi$ in $O(n^4(\log n)^2)$ bit operations.

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, $\mathrm{tr}\,\pi$ reveals the structure of $\mathbb{Z}[\pi]$ 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, $\mathrm{tr}\,\pi$ reveals the structure of $\mathbb{Z}[\pi]$ 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 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

Representing endomorphisms

Now assume $\alpha = \phi_L \circ \cdots \circ \phi_1 \in \mathrm{End}(E)$ 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, meaning

$$\phi_i(x, y) = \left(\frac{u_i(x)}{v_i(x)}, c \left(\frac{u_i(x)}{v_i(x)} \right)' y \right),$$

where $v_i(x) = \prod_{0 \neq P \in \ker \phi_i} (x - x(P))$.

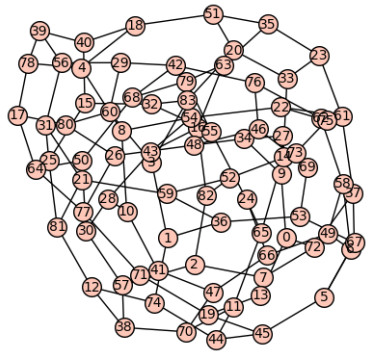


Figure: $G(313, 2)$, The 2-isogeny graph of supersingular elliptic curves in characteristic 313

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 $0 \le c < \ell$ 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) $\operatorname{tr}\pi = \pm 2p^a$ so $\pi = [\pm p^a]$, 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 $E/\mathbb{F}_{p^2}$ is supersingular, $j(E) \neq 0, 1728$.

The SEA algorithm for supersingular endomorphisms

Suppose $E/\mathbb{F}_{p^2}$ is supersingular, $j(E) \neq 0, 1728$. 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 $\mathbb{F}_{p^2}$ with $j(E) \neq 0, 1728$, let $n = \lceil \log p \rceil$, and let $\ell = O(n)$ be an odd prime. Let $d = \max\{\deg \phi_i\}$. Assume that $L \log d = O(n)$. 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, $\mathsf{M}(n) = O(n \log n)$ (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 $\mathbb{F}_{p^2}$ with $j(E) \neq 0, 1728$. Let $n = \lceil \log p \rceil$. Assume that $L \log d = O(n)$. Then $\operatorname{tr} \alpha$ can be computed in an expected $O(n^4 (\log n)^2 + dLn^3)$ 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)

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

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)

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

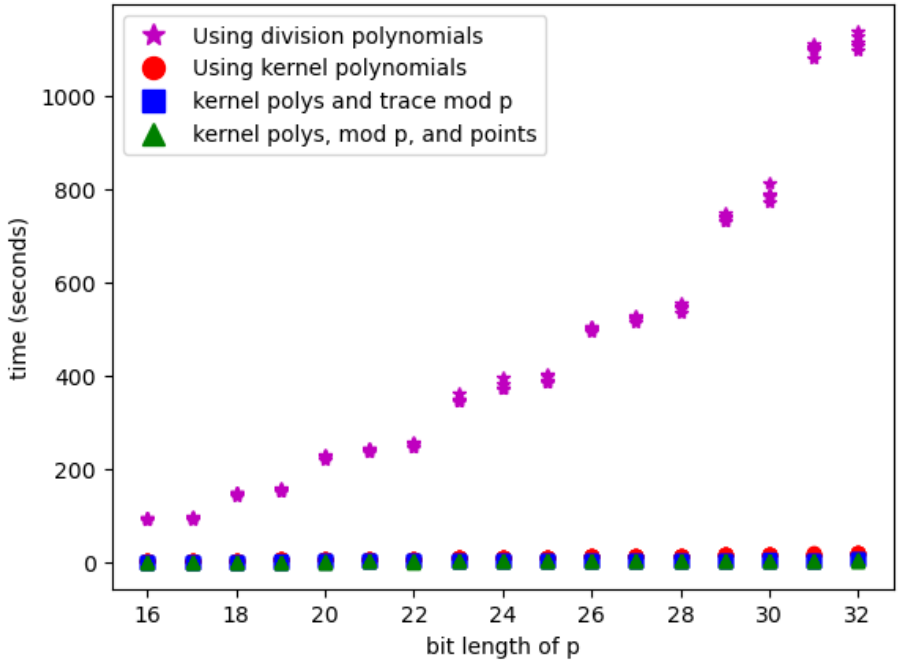
We can "read off" c_α from α: for separable α, we have

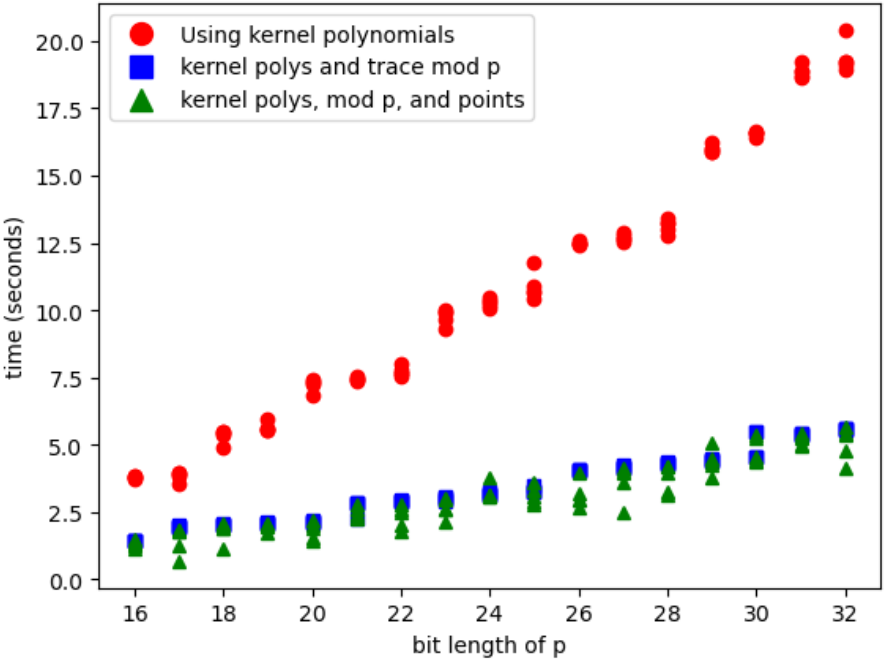
$$\alpha(x, y) = \left(\frac{N(x)}{D(x)}, \; c_\alpha \cdot \left(\frac{N(x)}{D(x)} \right)' y \right)$$

Timings

Implemented in sagemath. To demonstrate the asymptotic speedups offered:

1. For each $b \in [16, \ldots, 32]$, repeat 5 times:
   - 1.1 Compute random b-bit prime p, pseudorandom supersingular $E/\mathbb{F}_{p^2}$, and endomorphism $\alpha \in \mathrm{End}(E)$ of degree $\approx p^4$
   - 1.2 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
time (seconds)
0
200
400
600
800
1000
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?