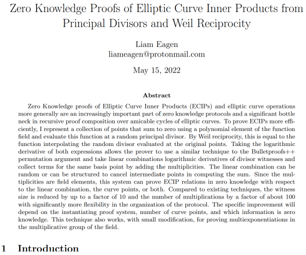
A gentle introduction to Hasse's theorem

Ariel Gabizon

Aztec

Motivation

Opening the black-box of elliptic curves can bring interesting results.



Zero Knowledge Proofs of Elliptic Curve Inner Products from Principal Divisors and Weil Reciprocity

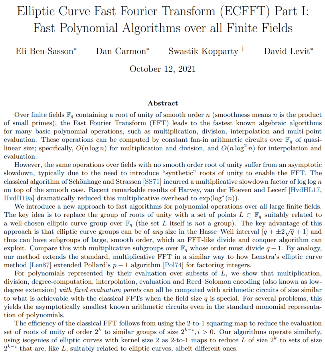
Liam Eagen
liameagen@protonmail.com

May 15, 2022

Abstract

Zero Knowledge proofs of Elliptic Curve Inner Products (ECIPs) and elliptic curve operations more generally are an increasingly important part of zero knowledge protocols and a significant bottle neck in recursive proof composition over amicable cycles of elliptic curves. To prove ECIPs more efficiently, I represent a collection of points that sum to zero using a polynomial element of the function field and evaluate this function at a random principal divisor. By Weil reciprocity, this is equal to the function interpolating the random divisor evaluated at the original points. Taking the logarithmic derivative of both expressions allows the prover to use a similar technique to the Bulletproofs++ permutation argument and take linear combinations logarithmic derivatives of divisor witnesses and collect terms for the same basis point by adding the multiplicities. The linear combination can be random or can be structured to cancel intermediate points in computing the sum. Since the multiplicities are field elements, this system can prove ECIP relations in zero knowledge with respect to the linear combination, the curve points, or both. Compared to existing techniques, the witness size is reduced by up to a factor of 10 and the number of multiplications by a factor of about 100 with significantly more flexibility in the organization of the protocol. The specific improvement will depend on the instantiating proof system, number of curve points, and which information is zero knowledge. This technique also works, with small modification, for proving multiexponentiations in the multiplicative group of the field.

1 Introduction



Elliptic Curve Fast Fourier Transform (ECFFT) Part I:
Fast Polynomial Algorithms over all Finite Fields

Eli Ben-Sasson* Dan Carmon* Swastik Kopparty † David Levit*

October 12, 2021

Abstract

Over finite fields $\mathbb{F}_q$ containing a root of unity of smooth order n (smoothness means n is the product of small primes), the Fast Fourier Transform (FFT) leads to the fastest known algebraic algorithms for many basic polynomial operations, such as multiplication, division, interpolation and multi-point evaluation. These operations can be computed by constant fan-in arithmetic circuits over $\mathbb{F}_q$ of quasi-linear size; specifically, $O(n \log n)$ for multiplication and division, and $O(n \log^2 n)$ for interpolation and evaluation.

However, the same operations over fields with no smooth order root of unity suffer from an asymptotic slowdown, typically due to the need to introduce “synthetic” roots of unity to enable the FFT. The classical algorithm of Schönhage and Strassen [SS71] incurred a multiplicative slowdown factor of $\log \log n$ on top of the smooth case. Recent remarkable results of Harvey, van der Hoeven and Lecerf [HvdHL17, HvdH19a] dramatically reduced this multiplicative overhead to $\exp(\log^*(n))$.

We introduce a new approach to fast algorithms for polynomial operations over all large finite fields. The key idea is to replace the group of roots of unity with a set of points $L \subset \mathbb{F}_q$ suitably related to a well-chosen elliptic curve group over $\mathbb{F}_q$ (the set L itself is *not* a group). The key advantage of this approach is that elliptic curve groups can be of *any* size in the Hasse–Weil interval $[q + \pm 2\sqrt{q} + 1]$ and thus can have subgroups of large, smooth order, which an FFT-like divide and conquer algorithm can exploit. Compare this with multiplicative subgroups over $\mathbb{F}_q$ whose order must divide $q - 1$. By analogy, our method extends the standard, multiplicative FFT in a similar way to how Lenstra's elliptic curve method [Len87] extended Pollard's $p - 1$ algorithm [Pol74] for factoring integers.

For polynomials represented by their evaluation over subsets of L, we show that multiplication, division, degree-computation, interpolation, evaluation and Reed–Solomon encoding (also known as low-degree extension) *with fixed evaluation points* can all be computed with arithmetic circuits of size similar to what is achievable with the classical FFTs when the field size q is special. For several problems, this yields the asymptotically smallest known arithmetic circuits even in the standard monomial representation of polynomials.

The efficiency of the classical FFT follows from using the 2-to-1 squaring map to reduce the evaluation set of roots of unity of order 2^k to similar groups of size $2^{k-i}, i > 0$. Our algorithms operate similarly, using isogenies of elliptic curves with kernel size 2 as 2-to-1 maps to reduce L of size 2^k to sets of size 2^{k-i} that are, like L, suitably related to elliptic curves, albeit different ones.

Curve E over $\mathbb{F}_p$.

$$y^2 = x^3 + ax + b$$

Curve E over $\mathbb{F}_p$.

$$y^2 = x^3 + ax + b$$

N := number of points over $\mathbb{F}_p$.

Curve E over $\mathbb{F}_p$.

$$y^2 = x^3 + ax + b$$

N := number of points over $\mathbb{F}_p$.

- $N \geq 1$ - cause always have point at infinity.

Curve E over $\mathbb{F}_p$.

$$y^2 = x^3 + ax + b$$

$N :=$ number of points over $\mathbb{F}_p$.

- $N \geq 1$ - cause always have point at infinity.
- $N \leq 2p + 1$ - cause at most two y's for each $x \in \mathbb{F}_p$.

Curve E over $\mathbb{F}_p$.

$$y^2 = x^3 + ax + b$$

$N :=$ number of points over $\mathbb{F}_p$.

- $N \geq 1$ - cause always have point at infinity.
- $N \leq 2p + 1$ - cause at most two y's for each $x \in \mathbb{F}_p$.

Hasse's thm: Set $a := p + 1 - N$. Then $|a| \leq 2\sqrt{p}$.

Hasse's thm is foundational for EC cryptography

Hasse's thm: $|\mathbf{p}+\mathbf{1}-\mathbf{N}| \leq \mathbf{2}\sqrt{\mathbf{p}}$.

Want $\mathbf{E}$ *of size* $\mathbf{N} \sim \mathbf{2}^{\mathbf{m}}$*?*

Hasse's thm is foundational for EC cryptography

Hasse's thm: $|\mathbf{p}+\mathbf{1}-\mathbf{N}| \leq \mathbf{2}\sqrt{\mathbf{p}}$.

Want $\mathbf{E}$ *of size* $\mathbf{N} \sim \mathbf{2}^{\mathbf{m}}$*?*

Just pick prime $\mathbf{p}$ with $\mathbf{m}$ bits, and take *any* elliptic curve $\mathbf{E}$ over $\mathbb{F}_{\mathbf{p}}$.

Hasse's thm is foundational for EC cryptography

Hasse's thm: $|\mathbf{p} + \mathbf{1} - \mathbf{N}| \leq \mathbf{2}\sqrt{\mathbf{p}}$.

Want $\mathbf{E}$ *of size* $\mathbf{N} \sim \mathbf{2^m}$*?*

Just pick prime $\mathbf{p}$ with $\mathbf{m}$ bits, and take *any* elliptic curve $\mathbf{E}$ over $\mathbb{F}_{\mathbf{p}}$.

The proof begins with some junior-high algebra

set $a := p + 1 - N$.
and $L(X) := X^2 - aX + p$

The proof begins with some junior-high algebra

set $a := p + 1 - N$.
and $L(X) := X^2 - aX + p$

Enough to show L's roots are not in $\mathbb{R}$:

The proof begins with some junior-high algebra

set $\mathbf{a} := \mathbf{p} + \mathbf{1} - \mathbf{N}$.
and $\mathbf{L}(\mathbf{X}) := \mathbf{X}^2 - \mathbf{a}\mathbf{X} + \mathbf{p}$

Enough to show $\mathbf{L}$'s roots are not in $\mathbb{R}$:

It would imply:

$$\boldsymbol{\Delta} = \mathbf{a}^2 - \mathbf{4p} < \mathbf{0} \rightarrow |\mathbf{a}| < \mathbf{2}\sqrt{\mathbf{p}}$$

The proof begins with some junior-high algebra

set $a := p + 1 - N$.
and $L(X) := X^2 - aX + p$

Enough to show L's roots are not in $\mathbb{R}$:

It would imply:

$$\Delta = a^2 - 4p < 0 \to |a| < 2\sqrt{p}$$

$a := p + 1 - N$. $L(X) = X^2 - aX + p$

$a := p + 1 - N$. $L(X) = X^2 - aX + p$

Claim: When p is prime, L's roots cannot be in $\mathbb{Z}$.

$a := p + 1 - N$. $L(X) = X^2 - aX + p$

Claim: When p is prime, L's roots cannot be in $\mathbb{Z}$.

proof: Write $L(X) = (X - \omega_1)(X - \omega_2)$. We have $p = \omega_1 \cdot \omega_2$, $a = \omega_1 + \omega_2$.

$a := p + 1 - N$. $L(X) = X^2 - aX + p$

Claim: When p is prime, L's roots cannot be in $\mathbb{Z}$.

proof: Write $L(X) = (X - \omega_1)(X - \omega_2)$. We have $p = \omega_1 \cdot \omega_2$, $a = \omega_1 + \omega_2$.

Only options for $\{\omega_1, \omega_2\}$:

$a := p + 1 - N$. $L(X) = X^2 - aX + p$

Claim: When p is prime, L's roots cannot be in $\mathbb{Z}$.

proof: Write $L(X) = (X - \omega_1)(X - \omega_2)$. We have $p = \omega_1 \cdot \omega_2$, $a = \omega_1 + \omega_2$.

Only options for $\{\omega_1, \omega_2\}$:

- $\{1, p\}$, but then $a = p + 1 \Rightarrow N = 0$.

$a := p + 1 - N$. $L(X) = X^2 - aX + p$

Claim: When p is prime, L's roots cannot be in $\mathbb{Z}$.

proof: Write $L(X) = (X - \omega_1)(X - \omega_2)$. We have $p = \omega_1 \cdot \omega_2$, $a = \omega_1 + \omega_2$.

Only options for $\{\omega_1, \omega_2\}$:

- $\{1, p\}$, but then $a = p + 1 \Rightarrow N = 0$.
- $\{-1, -p\}$, but then $N = 2p + 2$.

Elliptic curve endomorphisms

Homomorphisms $\psi : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p)$ *that "know"*
E *is an EC*

Elliptic curve endomorphisms

Homomorphisms $\psi : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p)$ *that "know"* E *is an EC*

- $\psi(P + Q) = \psi(P) + \psi(Q)$
- $\psi(0) = 0$

Elliptic curve endomorphisms

Homomorphisms $\psi : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p)$ *that "know"* E *is an EC*

- $\psi(P + Q) = \psi(P) + \psi(Q)$
- $\psi(\mathbf{0}) = \mathbf{0}$
- When $P = (x, y)$,
  $\psi(x, y) = (r(x, y), s(x, y))$ for some rational functions r, s over $\mathbb{F}_p$.

Elliptic curve endomorphisms

Homomorphisms $\psi : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p)$ *that "know"* E *is an EC*

- $\psi(P + Q) = \psi(P) + \psi(Q)$
- $\psi(\mathbf{0}) = \mathbf{0}$
- When $P = (x, y)$,
  $\psi(x, y) = (r(x, y), s(x, y))$ for some rational functions r, s over $\mathbb{F}_p$.

EC endomorphisms are a *ring* **END**$_E$:
$\psi_1 \cdot \psi_2(P) := \psi_1(\psi_2(P))$.

Elliptic curve endomorphisms

Example 1: $\mathbf{P} - > \mathbf{c} \cdot \mathbf{P}$ for integer c.

Elliptic curve endomorphisms

Example 1: $\mathbf{P} -> \mathbf{c} \cdot \mathbf{P}$ for integer c.

The Frobenius endomorphism

Example 2: $\phi(x, y) = (x^p, y^p)$.

The Frobenius endomorphism

Example 2: $\phi(x, y) = (x^p, y^p)$.

- Not the identity map because we're looking at points over $\overline{\mathbb{F}}_p$.

The Frobenius endomorphism

Example 2: $\phi(x, y) = (x^p, y^p)$.

- Not the identity map because we're looking at points over $\overline{\mathbb{F}}_p$.
- It's really an endomorphism, basically cause $(A + B)^p = A^p + B^p$:

The Frobenius endomorphism

Example 2: $\phi(x, y) = (x^p, y^p)$.

- Not the identity map because we're looking at points over $\overline{\mathbb{F}}_p$.
- It's really an endomorphism, basically cause $(A + B)^p = A^p + B^p$:

$$y^2 - x^3 - ax - b = 0$$

The Frobenius endomorphism

Example 2: $\phi(x, y) = (x^p, y^p)$.

- Not the identity map because we're looking at points over $\overline{\mathbb{F}}_p$.
- It's really an endomorphism, basically cause $(A + B)^p = A^p + B^p$:

$$y^2 - x^3 - ax - b = 0$$

$$\Rightarrow \left(y^2 - x^3 - ax - b\right)^p = 0$$

The Frobenius endomorphism

Example 2: $\phi(x, y) = (x^p, y^p)$.

- Not the identity map because we're looking at points over $\overline{\mathbb{F}}_p$.
- It's really an endomorphism, basically cause $(A + B)^p = A^p + B^p$:

$$y^2 - x^3 - ax - b = 0$$

$$\Rightarrow \left(y^2 - x^3 - ax - b\right)^p = 0$$

$$\Rightarrow (y^p)^2 - (x^p)^3 - a(x^p) - b = 0$$

The Frobenius endomorphism

Example 2: $\phi(x, y) = (x^p, y^p)$.

- Not the identity map because we're looking at points over $\overline{\mathbb{F}}_p$.
- It's really an endomorphism, basically cause $(A + B)^p = A^p + B^p$:

$$y^2 - x^3 - ax - b = 0$$

$$\Rightarrow \left(y^2 - x^3 - ax - b\right)^p = 0$$

$$\Rightarrow (y^p)^2 - (x^p)^3 - a(x^p) - b = 0$$

$$\Rightarrow (x^p, y^p) \in E.$$

$\phi(x, y) = (x^p, y^p)$. $L(X) = X^2 - aX + p$.

Lemma: ϕ is a "root" of L.

$\phi(x, y) = (x^p, y^p)$. $L(X) = X^2 - aX + p$.

Lemma: ϕ is a "root" of L.

I.e., $\phi^2 - a \cdot \phi + p$ is the all zero map.

$\phi(x, y) = (x^p, y^p)$. $L(X) = X^2 - aX + p$.

Lemma: ϕ is a "root" of L.

I.e., $\phi^2 - a \cdot \phi + p$ is the all zero map.

i.e., $\forall (x, y) \in E$:

$$(x^{p^2}, y^{p^2}) - a \cdot (x^p, y^p) + p \cdot (x, y) = \mathbf{0}_E$$

$\phi(x, y) = (x^p, y^p)$. $L(X) = X^2 - aX + p$.

Lemma: ϕ is a “root” of L.

I.e., $\phi^2 - a \cdot \phi + p$ is the all zero map.

i.e., $\forall (x, y) \in E$:

$$(x^{p^2}, y^{p^2}) - a \cdot (x^p, y^p) + p \cdot (x, y) = \mathbf{0}_E$$

maybe interesting for snark optimizers:
$p \cdot (x, y) = a \cdot (x^p, y^p) - (x^{p^2}, y^{p^2})$

$\mathbf{\Phi}$ is a “root” of $\mathbf{L}$. Left to show it corresponds to a complex imaginary number that is also a root of $\mathbf{L}$.

Φ is a "root" of $\mathbf{L}$. Left to show it corresponds to a complex imaginary number that is also a root of $\mathbf{L}$.

This is where *complex multiplication* comes in.

Complex multiplication over characteristic p

Thm: There is an isomorphism $\mathbf{T}$ from $\mathbf{END}_E$ to a ring $\mathbf{R}_E = \mathbb{Z} + \mathbb{Z} \cdot \mathbf{d}$, for some $\mathbf{d} \in \mathbb{C} \setminus \mathbb{R}$.

Complex multiplication over characteristic p

Thm: There is an isomorphism T from $\mathbf{END_E}$ to a ring $\mathbf{R_E} = \mathbb{Z} + \mathbb{Z} \cdot \mathbf{d}$, for some $\mathbf{d} \in \mathbb{C} \setminus \mathbb{R}$.

$$\mathsf{L}(\mathsf{T}(\phi)) = \mathsf{T}(\mathsf{L}(\phi)) = \mathsf{T}(\mathbf{0}_{\mathbf{END_E}}) = \mathbf{0}$$

Complex multiplication over characteristic p

Thm: There is an isomorphism T from $\mathbf{END_E}$ to a ring $\mathbf{R_E} = \mathbb{Z} + \mathbb{Z} \cdot \mathbf{d}$, for some $\mathbf{d} \in \mathbb{C} \setminus \mathbb{R}$.

$$\mathbf{L}(\mathsf{T}(\phi)) = \mathsf{T}(\mathbf{L}(\phi)) = \mathsf{T}(\mathbf{0}_{\mathbf{END_E}}) = \mathbf{0}$$

So $\omega := \mathsf{T}(\phi)$ is a root of $\mathbf{L}$!

Complex multiplication over characteristic p

Thm: There is an isomorphism T from $\mathbf{END_E}$ to a ring $\mathbf{R_E} = \mathbb{Z} + \mathbb{Z} \cdot \mathbf{d}$, for some $\mathbf{d} \in \mathbb{C} \setminus \mathbb{R}$.

$$L(\mathsf{T}(\phi)) = \mathsf{T}(L(\phi)) = \mathsf{T}(\mathbf{0}_{\mathbf{END_E}}) = \mathbf{0}$$

So $\omega := \mathsf{T}(\phi)$ is a root of L!

We showed before $\omega \notin \mathbb{Z}$ so must have $\omega \notin \mathbb{R}$ and we're done!

Historical context

Where did this last thm come from? Torus/curve equivalence over complex numbers.

Historical context

Where did this last thm come from? Torus/curve equivalence over complex numbers.

$\mathbf{L}$ is related to the zeta function of the elliptic curve, and RH for curve actually shows $|\omega_1| = |\omega_2| = \sqrt{p}$.

Sources:

- *Elliptic curves number theory and cryptography* - Lawrence C. Washington.
- *The Riemann Hypothesis in Characteristic* $\mathbf{p}$ *in Historical Perspective* - Peter Roquette

Thanks to Aztec crypto team for comments!