

Computing isogenies in small characteristics

L. De Feo

Projet TANC, LIX, École Polytechnique, Paris, France

June 19, 2009
Université de Bordeaux 1

Elliptic curves

Elliptic curves

- (Finite) field \mathbb{K} , with closure $\bar{\mathbb{K}}$,
- Weierstrass form: let $a, b \in \mathbb{K}$,

$$E : Y^2 = X^3 + aX + b$$

- $E(\mathbb{K})$ set of \mathbb{K} -rational points,
- $E(\mathbb{K})$ is a (finite) group. May be used for crypto.

j -invariant

$$j(E) = \frac{1728(4a)^3}{16(4a^3 + 27b^2)}$$

Two elliptic curves are isomorphic over $\bar{\mathbb{K}}$ iff they have the same j -invariant.

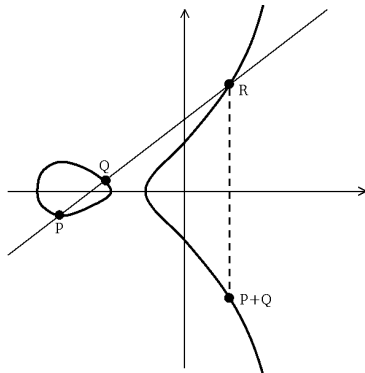


Figure: point addition on a Weierstrass curve over \mathbb{R}

Isogenies

$$E(\bar{\mathbb{K}}) \xrightarrow{\mathcal{I}} E'(\bar{\mathbb{K}})$$

Isogeny

- Rational map: $\mathcal{I}(X, Y) = \left(\frac{a(X, Y)}{b(X, Y)}, \frac{c(X, Y)}{d(X, Y)} \right),$
- onto, finite kernel, $\deg \mathcal{I} = [\bar{\mathbb{K}}(E') : \mathcal{I}^* \bar{\mathbb{K}}(E)],$
- group morphism: $\mathcal{I}(P + Q) = \mathcal{I}(P) + \mathcal{I}(Q), \quad \mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$

Examples

Multiplication

$$\begin{aligned} [m] : E(\bar{\mathbb{K}}) &\rightarrow E(\bar{\mathbb{K}}) \\ P &\mapsto [m]P \end{aligned}$$

$$\deg[m] = m^2, \quad \ker \mathcal{I} = E[m].$$

Isogenies

$$E(\bar{\mathbb{K}}) \xrightarrow{\mathcal{I}} E'(\bar{\mathbb{K}})$$

Isogeny

- Rational map: $\mathcal{I}(X, Y) = \left(\frac{a(X, Y)}{b(X, Y)}, \frac{c(X, Y)}{d(X, Y)} \right),$
- onto, finite kernel, $\deg \mathcal{I} = [\bar{\mathbb{K}}(E') : \mathcal{I}^* \bar{\mathbb{K}}(E)],$
- group morphism: $\mathcal{I}(P + Q) = \mathcal{I}(P) + \mathcal{I}(Q), \quad \mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$

Examples

Small Frobenius map

$$\begin{aligned} \varphi_p : E(\bar{\mathbb{K}}) &\rightarrow E^{(p)}(\bar{\mathbb{K}}) \\ (X, Y) &\mapsto (X^p, Y^p) \end{aligned}$$

where $E^{(p)} : Y^2 = X^3 + a^p X + b^p$ if $p = \text{char}(\mathbb{K})$,
 $\deg \varphi_p = p$, $\ker \varphi_p = \{\mathcal{O}\}.$

Isogenies

$$E(\bar{\mathbb{K}}) \xrightarrow{\mathcal{I}} E'(\bar{\mathbb{K}})$$

Isogeny

- Rational map: $\mathcal{I}(X, Y) = \left(\frac{a(X, Y)}{b(X, Y)}, \frac{c(X, Y)}{d(X, Y)} \right),$
- onto, finite kernel, $\deg \mathcal{I} = [\bar{\mathbb{K}}(E') : \mathcal{I}^* \bar{\mathbb{K}}(E)],$
- group morphism: $\mathcal{I}(P + Q) = \mathcal{I}(P) + \mathcal{I}(Q), \quad \mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$

Examples

Frobenius endomorphism

$$\begin{aligned} \varphi_q : E(\bar{\mathbb{K}}) &\rightarrow E(\bar{\mathbb{K}}) \\ (X, Y) &\mapsto (X^q, Y^q) \end{aligned}$$

if $\mathbb{K} = \mathbb{F}_q$ then $E^{(q)} = E$, $\deg \varphi_q = q$, $\ker \varphi_q = \{\mathcal{O}\}.$

Isogenies

$$E(\bar{\mathbb{K}}) \xrightarrow{\mathcal{I}} E'(\bar{\mathbb{K}})$$

Isogeny

- Rational map: $\mathcal{I}(X, Y) = \left(\frac{a(X, Y)}{b(X, Y)}, \frac{c(X, Y)}{d(X, Y)} \right),$
- onto, finite kernel, $\deg \mathcal{I} = [\bar{\mathbb{K}}(E') : \mathcal{I}^* \bar{\mathbb{K}}(E)],$
- group morphism: $\mathcal{I}(P + Q) = \mathcal{I}(P) + \mathcal{I}(Q), \quad \mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$

Examples

Separable isogenies

$$\mathcal{I}(X, Y) = \left(\frac{g(X)}{h^2(X)}, cY \left(\frac{g(X)}{h^2(X)} \right)' \right)$$

$$\deg \mathcal{I} = \# \ker \mathcal{I} \approx \deg h.$$

Dual isogeny

$$\begin{array}{ccc} E & \xrightarrow{\mathcal{I}} & E' \\ & \searrow [m] & \downarrow \hat{\mathcal{I}} \\ & & E \end{array}$$

Theorem (Dual isogeny)

\mathcal{I} of degree m , there is an unique dual isogeny $\hat{\mathcal{I}}$ s.t.

$$\hat{\mathcal{I}} \circ \mathcal{I} = [m]_E$$

$$\mathcal{I} \circ \hat{\mathcal{I}} = [m]_{E'}$$

Examples

- $[p] = V \circ \varphi_p$, V separable,
- m prime to p , $[m] = \hat{\mathcal{I}} \circ \mathcal{I}$ separable.

Modular polynomials

Theorem

Let H be a \mathbb{K} -rational finite subgroup of E , then there is a unique curve E' defined over \mathbb{K} and a separable isogeny $\mathcal{I} : E \rightarrow E'$ having kernel H .

$$0 \longrightarrow H \longrightarrow E \xrightarrow{\mathcal{I}} E' \longrightarrow 0$$

We note E/H for E' .

Modular polynomial $\Phi_\ell(X, Y)$

- $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ contains $\ell + 1$ cyclic subgroups of order ℓ ,
- there are $\ell + 1$ elliptic j -invariants (not necessarily in \mathbb{K}) ℓ -isogenous to E ,
- $\Phi_\ell(X, Y)$: minimal polynomial of the modular function $j(\ell\tau)$,
- $\Phi_\ell(j(E), j(E')) = 0$ iff E and E' are ℓ -isogenous,
- $\deg \Phi_\ell = \ell + 1$, (huge) integer coefficients.

SEA (see [Schoof '95])

Schoof

- $\varphi^2 - [t] \circ \varphi + [q] = 0$, compute $t \bmod \ell$ for primes $< O(\log q)$,
- computations done modulo division polynomial of degree $O(\ell^2)$.

Elkies

- $E[\ell]$ contains subgroups E_i of order ℓ ,
- E_1 defined in an extension of \mathbb{K} of degree dividing $\ell - 1$, find isogenous curve E/E_1 ,
- compute $\mathcal{I} : E \rightarrow E/E_1$, then $\deg \mathcal{I} = O(\ell)$,
- consider φ_{E_1} to find $t \bmod \ell$, computations done modulo \mathcal{I} .
- Works for half of the primes.

Atkin

- Works for the other half of the primes,
- uses simpler equation (in a field extension) $\varphi_{E_1} = [k]_{E_1}$.

Other applications

Cryptanalysis

- Proving hardness of discrete logarithm ([Jao, Miller, Venkatesan '05]).
- Move discrete logarithms to easier curves ([Gaudry, Hess, Smart '02]).
- Discrete logarithms in genus 3 ([Smith '08]).

Cryptography

- Speeding up point multiplication ([Gallant, Lambert, Vanstone '01]).
- Hide weak curves behind chains of isogenies ([Teske '06]).
- Define hash functions ([Charles, Lauter, Goren '09]).

Computing isogenies: which problem?

- Is there a \mathbb{K} -rational isogeny between E and E' ?
- Is there a degree ℓ isogeny between E and E' ?
- What are the curves ℓ -isogenous to E ?
- Given E and a subgroup H , find E/H and $\mathcal{I} : E \rightarrow E'$
- Given E and a prime ℓ , find E' ℓ -isogenous to E and $\mathcal{I} : E \rightarrow E'$.
- Given E , E' and ℓ , find, if it exists, an isogeny $\mathcal{I} : E \rightarrow E'$.

Computing isogenies: which problem?

- Is there a \mathbb{K} -rational isogeny between E and E' ? $\Leftrightarrow \#E(\mathbb{K}) = \#E'(\mathbb{K})$
- Is there a degree ℓ isogeny between E and E' ? $\Leftrightarrow \Phi_\ell(j(E), j(E')) = 0$
- What are the curves ℓ -isogenous to E ? factor $\Phi_\ell(j(E), Y)$
- Given E and a subgroup H , find E/H and $\mathcal{I} : E \rightarrow E'$ Vélu formulae
- Given E and a prime ℓ , find E' ℓ -isogenous to E and $\mathcal{I} : E \rightarrow E'$.
- Given E , E' and ℓ , find, if it exists, an isogeny $\mathcal{I} : E \rightarrow E'$.

Computing isogenies: which problem?

- Is there a \mathbb{K} -rational isogeny between E and E' ? $\Leftrightarrow \#E(\mathbb{K}) = \#E'(\mathbb{K})$
- Is there a degree ℓ isogeny between E and E' ? $\Leftrightarrow \Phi_\ell(j(E), j(E')) = 0$
- What are the curves ℓ -isogenous to E ? factor $\Phi_\ell(j(E), Y)$
- Given E and a subgroup H , find E/H and $\mathcal{I} : E \rightarrow E'$ Vélu formulae
- Given E and a prime ℓ , find E' ℓ -isogenous to E and $\mathcal{I} : E \rightarrow E'$. (*)
- Given E , E' and ℓ , find, if it exists, an isogeny $\mathcal{I} : E \rightarrow E'$.

Computing isogenies: short history

Large characteristic (see [Bostan, Morain, Salvy, Schost 08])

'92 Elkies	$O(\ell^2)$
'92 Atkin	$O(\ell^2)$
'98 Elkies	$O(\ell^2)$
'08 Bostan, Morain, Salvy, Schost	$O(\ell)$

Small characteristic

'94 Couveignes I	$O(\ell^3)$
'96 $p = 2$, Lercier	$\Omega(\ell^3)$?
'96 Couveignes II (+ [D.F. '07])	$O(\ell^2)$

Outsiders

- Medium characteristic: [Joux, Lercier '06] $O(\ell^3)$
- p -adic BMSS08: [Lercier, Sirvent '09] $O(\ell^3)$
best algorithm for (*): $O(\ell^3)$

Couveignes II (or the lazy man's algorithm)

Recall...

- \mathcal{I} is a group morphism,
- \mathcal{I} is a rational fraction.

Interpolating an isogeny

- G a large enough subgroup,
- G' its image by \mathcal{I} ,
- interpolate over the points of G ,
- deduce the isogeny by rational reconstruction.

$$E(\bar{\mathbb{K}}) \supset G \xrightarrow{\mathcal{I}} G' \subset E'(\bar{\mathbb{K}})$$



$$A(X_P) = A(X_{P'}) \quad \text{for every } P \in G, P' = \mathcal{I}(P)$$



$$\frac{g(X)}{h^2(X)}$$

G is chosen to be $E[p^k]$

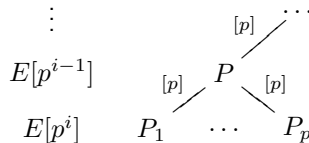
Disclaimer:

I do not mean that Couveignes is a lazy man!

p -torsion of ordinary elliptic curves

p^k -torsion

- $E[p^k] \simeq \mathbb{Z}/p^k\mathbb{Z}$,
- $\mathcal{I}(E[p^k]) = E'[p^k]$ iff $(\ell, p) = 1$,
- **points not necessarily defined over \mathbb{K} .**



Computing the p^i -torsion

- Let $P = (x_P, y_P) \in E[p^{i-1}]$ be known,
- recall $[p] = V \circ \varphi_p$, with V a degree p separable isogeny,
- V can be computed using Vélú formulae,
- solve $(\sqrt[p]{x_P}, \sqrt[p]{y_P}) = V(X, Y)$,
- **Voloch Formulae:** by a change of variables, this is equivalent to solve

$$X^p - X = \frac{\sqrt[p]{y_P \beta(x_P)}}{h}$$

for some polynomial β and constant h .

Torsion tower

$$\begin{array}{c} \mathbb{U}_k \\ \left| \begin{array}{c} p \\ \vdots \\ \vdots \end{array} \right. \\ \mathbb{U}_{k-1} \\ \vdots \\ \mathbb{U}_{i_0+1} \\ \left| \begin{array}{c} p \\ \vdots \\ \vdots \end{array} \right. \\ \mathbb{U}_{i_0} = \mathbb{K} \\ \vdots \\ \mathbb{U}_1 \\ \left| \begin{array}{c} 1 \\ \vdots \end{array} \right. \\ \mathbb{U}_0 = \mathbb{K} \end{array}$$

Definition (p^k -torsion tower)

$(\mathbb{K} = \mathbb{U}_0, \dots, \mathbb{U}_k)$ is the tower of field extensions of minimal degree s.t. for any i

$$E[p^i] \subset E(\mathbb{U}_i).$$

Theorem (Structure of $(\mathbb{U}_0, \dots, \mathbb{U}_k)$)

There is a $i_0 \geq 1$ s.t. $\mathbb{U}_{i_0} = \mathbb{U}_1$ and for $i \geq i_0$

$$[\mathbb{U}_{i+1} : \mathbb{U}_i] = p.$$

And $[\mathbb{U}_1 : \mathbb{U}_0]$ divides $p - 1$. For the sake of simplicity, we will sometimes assume $[\mathbb{U}_1 : \mathbb{U}_0] = 1$, some other times $[\mathbb{U}_1 : \mathbb{U}_0] = p - 1$.

Summarizing

Couveignes' algorithm

- ① Compute a p -torsion point of E ,
- ② repeatedly apply Voloch formulae to compute P , a p^k -torsion point of E ,
- ③ do the same to compute P' , a p^k -torsion point of E' ,
- ④ for $i \in [1, \dots, p^k - 1]$, i prime to p
 - ① interpolate the polynomial that sends P over $[i]P'$,
 - ② deduce a rational fraction and check if its denominator is a square.

Informal cost analysis (supposing $i_0 = 1$)

- To have enough points $\phi(p^k) > 4\ell$, then $[\mathbb{U}_k : \mathbb{K}] = p^{k-1} \sim \ell$.
- Step 1 is easy, step 2 costs $O(p^k)$ operations in the tower.
- Step 3 requires factorisation in \mathbb{U}_k . Cost is $O(p^{3k})$ by linear algebra.
- Steps 5 and 6 have to be repeated $\phi(p^k)$ times.
- Step 5 interpolates a polynomial of degree $\phi(p^k)$ in a field of degree p^{k-1} . That is $O(p^{2k})$ by fast techniques. Step 6 is some GCDs in \mathbb{K} , cost is $O(p^k)$.

Summarizing

Couveignes' algorithm

- ① Compute a p -torsion point of E ,
- ② repeatedly apply Voloch formulae to compute P , a p^k -torsion point of E ,
- ③ do the same to compute P' , a p^k -torsion point of E' ,
- ④ for $i \in [1, \dots, p^k - 1]$, i prime to p
 - ① interpolate the polynomial that sends P over $[i]P'$,
 - ② deduce a rational fraction and check if its denominator is a square.

Informal cost analysis (supposing $i_0 = 1$)

- To have enough points $\phi(p^k) > 4\ell$, then $[\mathbb{U}_k : \mathbb{K}] = p^{k-1} \sim \ell$.
- Step 1 is easy, step 2 costs $O(p^k)$ operations in the tower.
- Step 3 requires factorisation in \mathbb{U}_k . Cost is $O(p^{3k})$ by linear algebra.
- Steps 5 and 6 have to be repeated $\phi(p^k)$ times.
- Step 5 interpolates a polynomial of degree $\phi(p^k)$ in a field of degree p^{k-1} . That is $O(p^{2k})$ by fast techniques. Step 6 is some GCDs in \mathbb{K} , cost is $O(p^k)$.
- Total cost is $O(p^{3k}) = O(\ell^3)$.

Let's stop being lazy!

Couveignes' algorithm

- ① Compute a p -torsion point of E ,
- ② repeatedly apply Voloch formulae to compute P , a p^k -torsion point of E ,
- ③ do the same to compute P' , a p^k -torsion point of E' ,
- ④ for $i \in [1, \dots, p^k - 1]$, i prime to p
 - ① interpolate the polynomial that sends P over $[i]P'$,
 - ② deduce a rational fraction and check if its denominator is a square.

Informal cost analysis (supposing $i_0 = 1$)

- Step 3 requires factorisation in \mathbb{U}_k . Cost is $O(p^{3k})$ by linear algebra.
- [Couveignes '00] gives an algorithm with cost $O(p^k)$ operations in the tower.

Artin-Schreier towers

Definition (Artin-Schreier polynomial)

\mathbb{K} a field of characteristic p , $\alpha \in \mathbb{K}$

$$X^p - X - \alpha$$

is an Artin-Schreier polynomial.

Theorem

\mathbb{K} finite. $X^p - X - \alpha$ irreducible $\Leftrightarrow \text{Tr}_{\mathbb{K}/\mathbb{F}_p}(\alpha) \neq 0$.

If $\eta \in \mathbb{K}$ is a root, then $\eta + 1, \dots, \eta + (p-1)$ are roots.

Definition (Artin-Schreier extension)

\mathcal{P} an irreducible Artin-Schreier polynomial.

$$\mathbb{L} = \mathbb{K}[X]/\mathcal{P}(X).$$

\mathbb{L}/\mathbb{K} is called an Artin-Schreier extension.

Artin-Schreier towers

$$\begin{array}{c} \mathbb{U}_k = \frac{\mathbb{U}_{k-1}[X_k]}{P_{k-1}(X_k)} \\ \left| \begin{array}{c} p \\ \mathbb{U}_{k-1} \\ \vdots \\ \mathbb{U}_{i_0+1} = \frac{\mathbb{U}_0[X_1]}{P_0(X_1)} \\ \left| \begin{array}{c} p \\ \mathbb{U}_{i_0} = \mathbb{K} = \frac{\mathbb{F}_p[X_0]}{Q(X_0)} \end{array} \end{array} \right. \end{array}$$

Towers over finite fields

$$P_i = X^p - X - \alpha_i$$

We say that $(\mathbb{U}_0, \dots, \mathbb{U}_k)$ is defined by $(\alpha_0, \dots, \alpha_{k-1})$ over \mathbb{U}_0 .

ANY separable extension of degree p can be expressed this way

Voloch formulae

Remark that Voloch formulae give rise to an Artin-Schreier tower:

$$X^p - X = \frac{\sqrt[p]{y_P \beta(x_p)}}{h}$$

Solving Artin-Schreier equations in Artin-Schreier towers

[Couveignes '00]

- Given $\alpha_i \in \mathbb{U}_i$ with $\text{Tr}(\alpha) = 0$ solves

$$X^p - X = \alpha_i \in \mathbb{U}_i.$$

- By a change of variables, this is equivalent to solve

$$X^p - X = \beta_i \in \mathbb{U}_{i-1}.$$

- Applies the formula recursively. Complexity is $O(p^i)$.

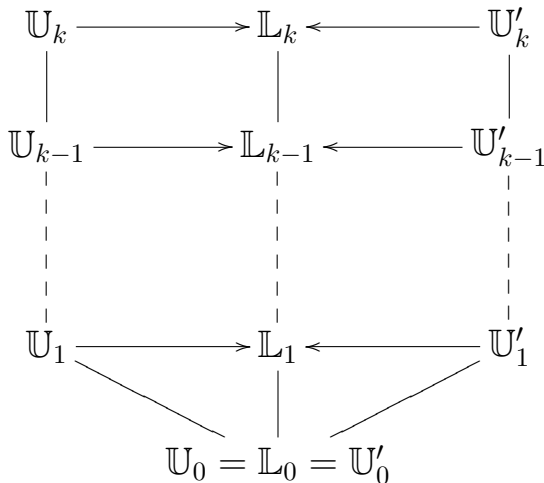
Isomorphisms of Artin-Schreier towers

- Equivalently, the algorithm finds an isomorphism between $(\mathbb{U}_0, \dots, \mathbb{U}_k)$ and the tower defined by $(\alpha_0, \dots, \alpha_{k-1})$.
- If there were a third tower $(\mathbb{L}_0, \dots, \mathbb{L}_k)$ with fast arithmetics...

\mathbb{U}_k
|
 \mathbb{U}_{k-1}
|
...
|
 \mathbb{U}_1
|
 \mathbb{U}_0

\mathbb{U}'_k
|
 \mathbb{U}'_{k-1}
|
...
|
 \mathbb{U}'_1
|
 \mathbb{U}'_0

Solving Artin-Schreier equations in Artin-Schreier towers



Let's stop being lazy!

Couveignes' algorithm

- ① Compute a p -torsion point of E ,
- ② repeatedly apply Voloch formulae to compute P , a p^k -torsion point of E ,
- ③ do the same to compute P' , a p^k -torsion point of E' ,
- ④ for $i \in [1, \dots, p^k - 1]$, i prime to p
 - ① interpolate the polynomial that sends P over $[i]P'$,
 - ② deduce a rational fraction and check if its denominator is a square.

Informal cost analysis (supposing $i_0 = 1$)

- To have enough points $\phi(p^k) > 4\ell$, then $[\mathbb{U}_k : \mathbb{K}] = p^{k-1} \sim \ell$.
- Step 1 is easy, step 2 costs $O(p^k)$ operations in the tower.
- Step 3 requires factorisation in \mathbb{U}_k . Cost is $O(p^k)$ ops by [Couveignes '00].
- Steps 5 and 6 have to be repeated $\phi(p^k)$ times.
- Step 5 interpolates a polynomial of degree $\phi(p^k)$ in a field of degree p^{k-1} . That is $O(p^{2k})$ operations. Step 6 is some GCDs in \mathbb{K} , cost is $O(p^k)$ ops.

Let's stop being lazy!

Couveignes' algorithm

- ① Compute a p -torsion point of E ,
- ② repeatedly apply Voloch formulae to compute P , a p^k -torsion point of E ,
- ③ do the same to compute P' , a p^k -torsion point of E' ,
- ④ for $i \in [1, \dots, p^k - 1]$, i prime to p
 - ① interpolate the polynomial that sends P over $[i]P'$,
 - ② deduce a rational fraction and check if its denominator is a square.

Informal cost analysis (supposing $i_0 = 1$)

- To have enough points $\phi(p^k) > 4\ell$, then $[\mathbb{U}_k : \mathbb{K}] = p^{k-1} \sim \ell$.
- Step 1 is easy, step 2 costs $O(p^k)$ operations in the tower.
- Step 3 requires factorisation in \mathbb{U}_k . Cost is $O(p^k)$ ops by [Couveignes '00].
- Steps 5 and 6 have to be repeated $\phi(p^k)$ times.
- Step 5 interpolates a polynomial of degree $\phi(p^k)$ in a field of degree p^{k-1} . That is $O(p^{2k})$ operations. Step 6 is some GCDs in \mathbb{K} , cost is $O(p^k)$ ops.
- But how much does it cost one operation?

Fast arithmetics in Artin-Schreier towers



Primitive towers ([D.F., Schost '09])

- Find special $(\gamma_0, \dots, \gamma_{k-1})$ that define a tower s.t. $\mathbb{L}_i = \mathbb{F}_p[x_i]$, where $x_i^p - x_i - \gamma_{i-1} = 0$.
- Use univariate representation over \mathbb{F}_p to perform fast arithmetics (FFT multiplication, Newton inversion, etc.).
- Use [Couveignes '00] algorithm to move to (U_0, \dots, U_k) .

Level embedding ([D.F., Schost '09])

- Express the morphisms between the levels to switch back to the multivariate representation.
- Going down is easy: bivariate reduction modulo $X_i^p - X_i - \gamma_{i-1}$.
- Going up much harder: trace formulae, truncated power series arithmetics, transposition principle.

Advertisement: FFAST

Download this C++ library at:

<http://www.lix.polytechnique.fr/Labo/Luca.De-Feo/FFAST>

Let's stop being lazy!

Couveignes' algorithm

- ① Compute a p -torsion point of E ,
- ② repeatedly apply Voloch formulae to compute P , a p^k -torsion point of E ,
- ③ do the same to compute P' , a p^k -torsion point of E' ,
- ④ for $i \in [1, \dots, p^k - 1]$, i prime to p
 - ① interpolate the polynomial that sends P over $[i]P'$,
 - ② deduce a rational fraction and check if its denominator is a square.

Formal cost analysis (supposing $i_0 = 1$, $\mathbb{K} = \mathbb{F}_q$)

- To have enough points $\phi(p^k) > 4\ell$, then $[\mathbb{U}_k : \mathbb{K}] = p^{k-1} \sim \ell$.
- Step 1 is easy, step 2 costs $O(p^k \log_p q)$ operations.
- Step 3 requires factorisation in \mathbb{U}_k . Cost is $O(p^k \log_p^2 q + \log_p^3 q)$.
- Steps 5 and 6 have to be repeated $\phi(p^k)$ times.
- Step 5 interpolates a polynomial of degree $\phi(p^k)$ in a field of degree p^{k-1} . That is $O(p^{2k} \log_p q)$. Step 6 is some GCDs in \mathbb{K} , cost is $O(p^k \log_p q)$.
- All costs in \mathbb{F}_p -operations.

Let's stop being lazy!

Couveignes' algorithm

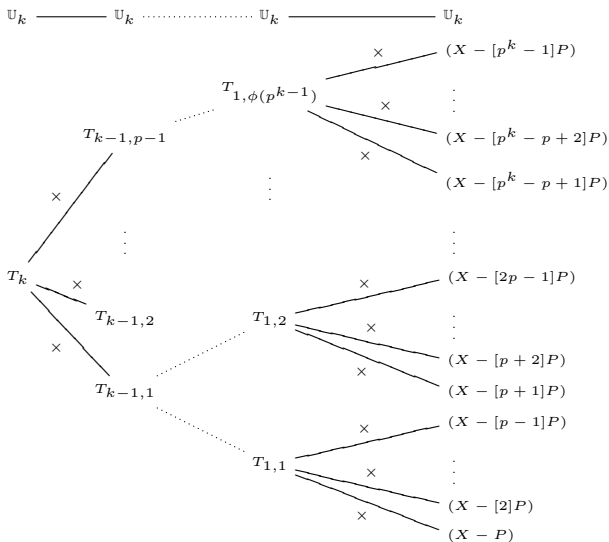
- ① Compute a p -torsion point of E ,
- ② repeatedly apply Voloch formulae to compute P , a p^k -torsion point of E ,
- ③ do the same to compute P' , a p^k -torsion point of E' ,
- ④ for $i \in [1, \dots, p^k - 1]$, i prime to p
 - ① interpolate the polynomial that sends P over $[i]P'$,
 - ② deduce a rational fraction and check if its denominator is a square.

Formal cost analysis (supposing $i_0 = 1$, $\mathbb{K} = \mathbb{F}_q$)

- To have enough points $\phi(p^k) > 4\ell$, then $[\mathbb{U}_k : \mathbb{K}] = p^{k-1} \sim \ell$.
- Step 1 is easy, step 2 costs $O(p^k \log_p q)$ operations.
- Step 3 requires factorisation in \mathbb{U}_k . Cost is $O(p^k \log_p^2 q + \log_p^3 q)$.
- Steps 5 and 6 have to be repeated $\phi(p^k)$ times.
- Step 5 interpolates a polynomial of degree $\phi(p^k)$ in a field of degree p^{k-1} . That is $O(p^{2k} \log_p q)$. Step 6 is some GCDs in \mathbb{K} , cost is $O(p^k \log_p q)$.
- All costs in \mathbb{F}_p -operations.

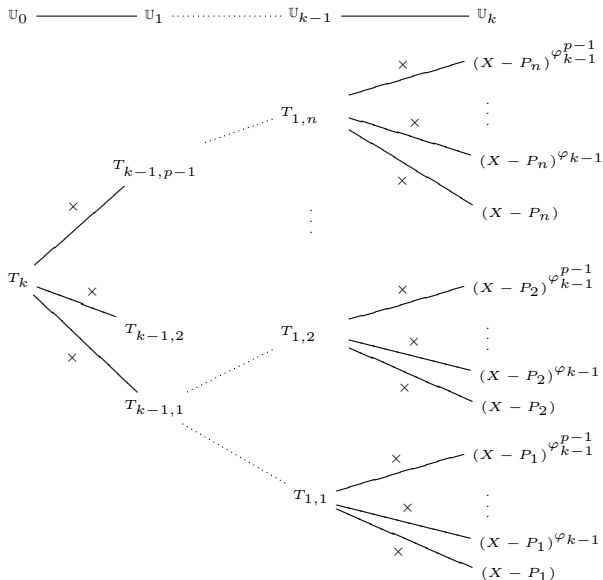
Beyond fast interpolation ([D.F. '07])

Subproduct
tree



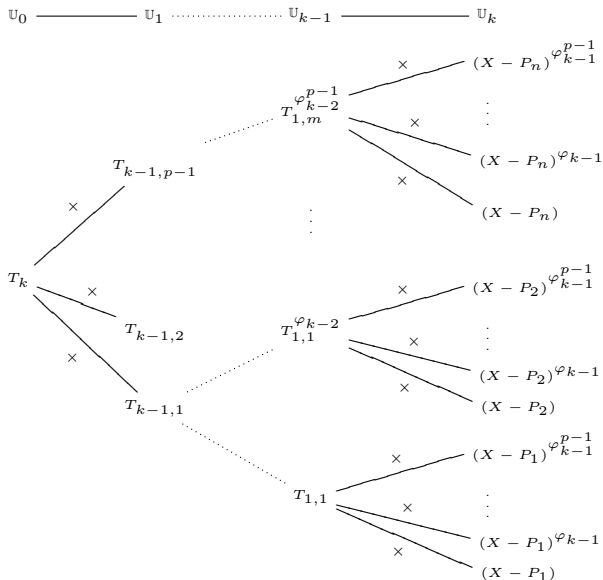
Beyond fast interpolation ([D.F. '07])

p^k -torsion tree

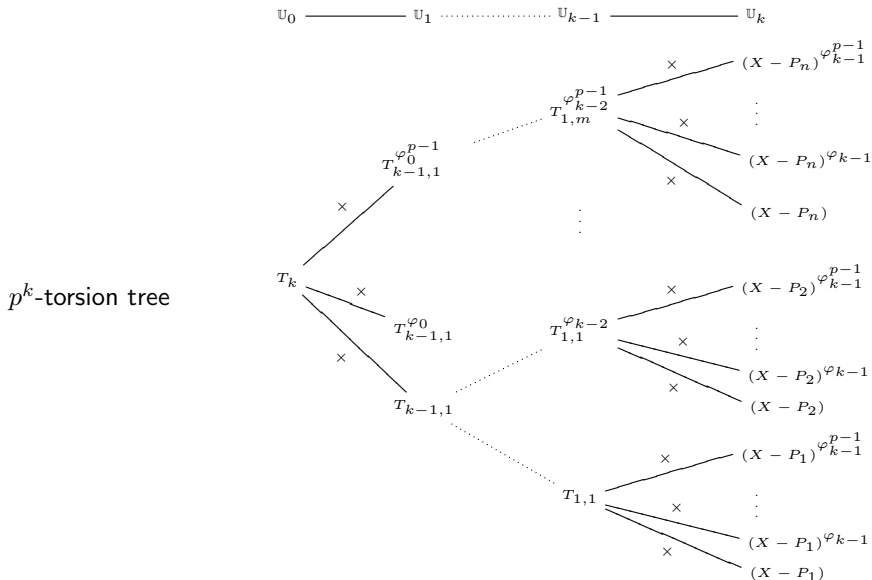


Beyond fast interpolation ([D.F. '07])

p^k -torsion tree



Beyond fast interpolation ([D.F. '07])



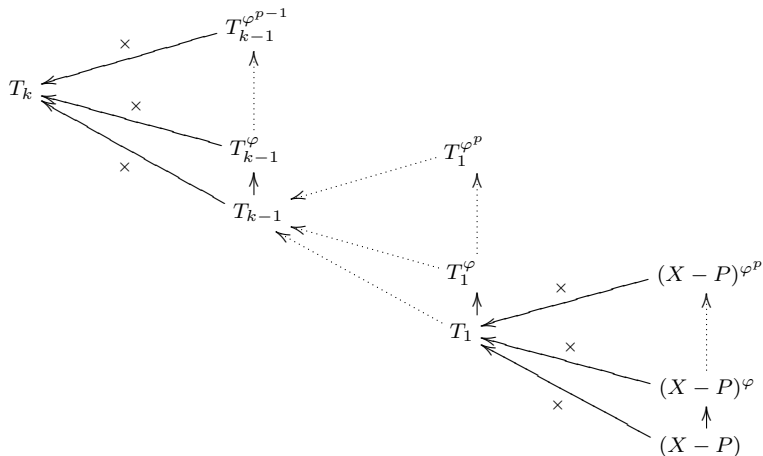
Beyond fast interpolation ([D.F. '07])

$$\deg T_k = p^k$$

$$\deg T_{k-1} = p^{k-1}$$

$$\deg T_1 = p$$

$$\deg(X - P) = 1$$



$$\mathbb{U}_0 \text{ ————— } \mathbb{U}_1 \text{ } \mathbb{U}_{k-1} \text{ ————— } \mathbb{U}_k$$

Summarizing

Couveignes' algorithm

- ① Compute a p -torsion point of E ,
- ② repeatedly apply Voloch formulae to compute P , a p^k -torsion point of E ,
- ③ do the same to compute P' , a p^k -torsion point of E' ,
- ④ for $i \in [1, \dots, p^k - 1]$, i prime to p
 - ① interpolate the polynomial that sends P over $[i]P'$,
 - ② deduce a rational fraction and check if its denominator is a square.

Formal cost analysis (supposing $i_0 = 1$, $\mathbb{K} = \mathbb{F}_q$)

- To have enough points $\phi(p^k) > 4\ell$, then $[\mathbb{U}_k : \mathbb{K}] = p^{k-1} \sim \ell$.
- Step 1 is easy, step 2 costs $O(p^k \log_p q)$ operations .
- Step 3 requires factorisation in \mathbb{U}_k . Cost is $O(p^k \log_p^2 q + \log_p^3 q)$.
- Steps 5 and 6 have to be repeated $\phi(p^k)$ times.
- Step 5 costs $O(p^k \log_p q)$ using the latter algorithm. Step 6 is some GCDs in \mathbb{K} , cost is $O(p^k \log_p q)$.
- Total cost is $O(\ell^2 \log_p q + \ell \log_p^2 q + \log_p^3 q)$.

Doing better than interpolation

Couveignes' algorithm

- for $i \in [1, \dots, p^k - 1]$, i prime to p
 - interpolate the polynomial that sends P over $[i]P'$,

Using modular composition

Let A_i be the polynomial with coefficients in \mathbb{F}_q sending P over $[i]P'$, then

$$A_1([j]P) = [j]P' \text{ for every } j.$$

Now let $\varphi_q(P') = [\lambda]P'$, then

$$A_1(\varphi_q([j]P)) = \varphi_q(A_1([j]P)) = \varphi_q([j]P') = [j][\lambda]P'.$$

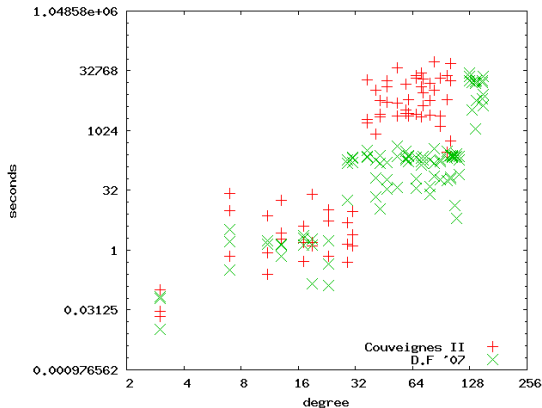
So $A_1 \circ \varphi_q = A_\lambda \bmod T_k$. Solving this is *modular composition*.

Modular composition

- Theoretical complexity $O(\ell \log_p q)$, practical complexity $O(\ell^2 \log_p^2 q) \dots$
- ... but still much faster than a single interpolation.

(Old) Timings

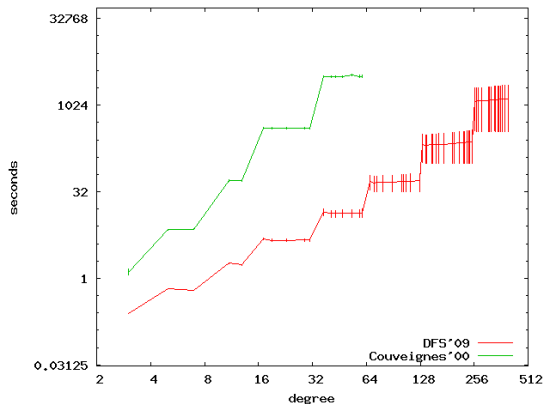
- Magma implementation,
- [Couveignes '96] vs. [D.F. '07],
- $\mathbb{K} = \mathbb{F}_{5^3}$.



	[Cou'96]	[D.F. '07]
Total time	65951	19864
Compute $E[p^k]$	0,06%	0,5%
Compute $E'[p^k]$	28%	89,5%
Interpolation	71%	9,5%

Timings

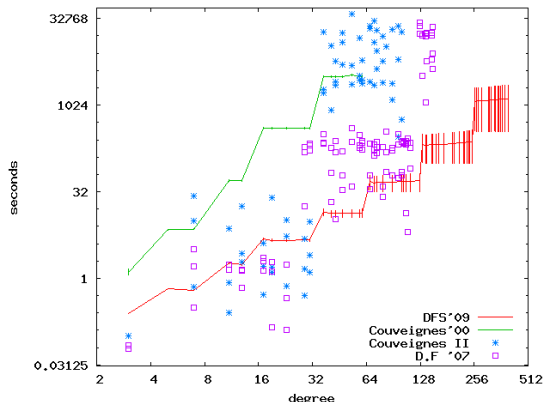
- NTL implementation of [D.F., Schost '09] vs. Magma implementation, of [Couveignes '00]
- $\mathbb{K} = \mathbb{F}_{2^{101}}$.



ℓ	$E[p^k]$	$E'[p^k]$	Interp	Step 6	ModComp	Avg tries	Avg loop time
31	1.3128	1.3128	1.1058	0.00218	0.00218	64	0.279
61	3.5454	3.5464	2.5236	0.00783	0.00900	128	2.154
127	9.2975	9.3026	5.6881	0.03147	0.03634	256	17.359
251	23.7984	23.7984	12.7251	0.12415	0.14519	512	137.902
397	59.7439	59.7579	28.3387	0.36822	0.58027	1024	971.254

Timings

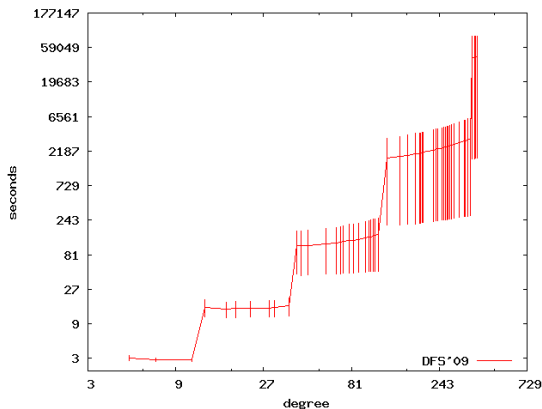
- NTL implementation of [D.F., Schost '09] vs. Magma implementation, of [Couveignes '00]
- $\mathbb{K} = \mathbb{F}_{2^{101}}$.



ℓ	$E[p^k]$	$E'[p^k]$	Interp	Step 6	ModComp	Avg tries	Avg loop time
31	1.3128	1.3128	1.1058	0.00218	0.00218	64	0.279
61	3.5454	3.5464	2.5236	0.00783	0.00900	128	2.154
127	9.2975	9.3026	5.6881	0.03147	0.03634	256	17.359
251	23.7984	23.7984	12.7251	0.12415	0.14519	512	137.902
397	59.7439	59.7579	28.3387	0.36822	0.58027	1024	971.254

Timings

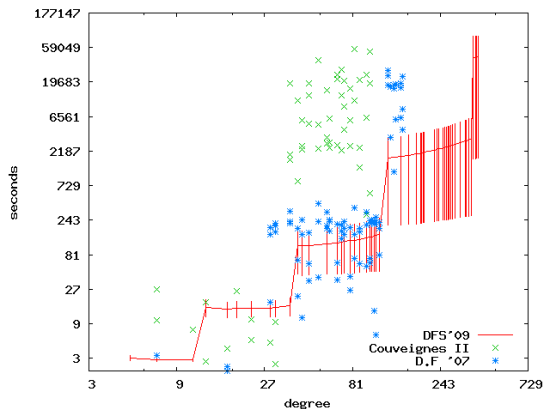
- NTL implementation of [D.F., Schost '09]
- $\mathbb{K} = \mathbb{F}_{3^{64}}$.



ℓ	$E[p^k]$	$E'[p^k]$	Interp	Step 6	ModComp	Avg tries	Avg loop time
11	0.6109	0.6109	0.4669	0.0194	0.0249	13	0.58
37	2.3946	2.3916	2.1066	0.1988	0.1381	40	13.48
113	9.8045	9.8055	8.5377	1.7712	0.8690	121	319.47
359	38.3292	38.3972	34.7147	17.5004	7.0088	364	8921.35
389	159.8280	159.5690	147.741	45.1558	69.9133	1093	125770.52

Timings

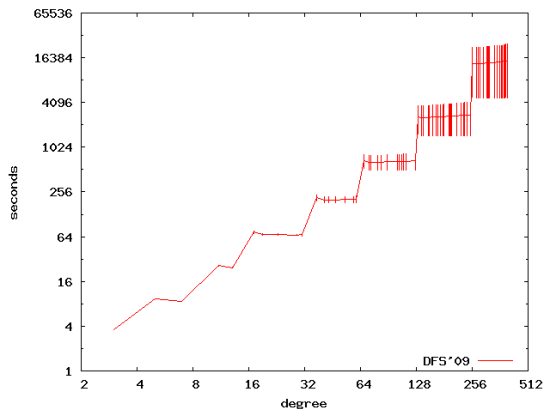
- NTL implementation of [D.F., Schost '09]
- $\mathbb{K} = \mathbb{F}_{3^{64}}$.



ℓ	$E[p^k]$	$E'[p^k]$	Interp	Step 6	ModComp	Avg tries	Avg loop time
11	0.6109	0.6109	0.4669	0.0194	0.0249	13	0.58
37	2.3946	2.3916	2.1066	0.1988	0.1381	40	13.48
113	9.8045	9.8055	8.5377	1.7712	0.8690	121	319.47
359	38.3292	38.3972	34.7147	17.5004	7.0088	364	8921.35
389	159.8280	159.5690	147.741	45.1558	69.9133	1093	125770.52

Record Timings!

- NTL implementation of [D.F., Schost '09]
- $\mathbb{K} = \mathbb{F}_{2^{1023}}$.



ℓ	$E[p^k]$	$E'[p^k]$	Interp	Step 6	ModComp	Avg tries	Avg loop time
31	21.182	21.174	11.597	0.0178	0.02541	64	2.768
61	58.656	58.665	26.826	0.0645	0.10398	128	21.576
127	154.357	154.296	61.202	0.2580	0.41578	256	172.503
251	383.773	383.861	138.428	0.9950	1.66120	512	1360.000
397	931.022	931.610	313.609	3.1819	6.73608	1024	10156.011

Ongoing work

Implementation (with F. Morain and E. Schost)





- SAGE porting of FFAST,
- SAGE porting of SEA + Lercier + Couveignes II,
- comparison with Lercier,
- comparison with Lercier-Sirvent.

Theory

- Try a p -adic version of Couveignes II + BMSS08 to reduce the number of tries in the final loop,
- Improve Lercier-Sirvent and make it the best algorithm for this problem.

Thanks

Bibliography

-  I. Blake, G. Seroussi & N. Smart
Elliptic Curves in Cryptography
LMS 265, Cambridge University Press, 1999
-  (edited by) I. Blake, G. Seroussi & N. Smart
Advances in Elliptic Curve Cryptography
LMS 317, Cambridge University Press, 2005
-  J.S. Milne.
Elliptic curves.
BookSurge Publishers, ISBN 1-4196-5257-5, 2006.
-  J.H. Silverman
The Arithmetic of Elliptic Curves
GTM 106, Springer-Verlag, 1986

Bibliography



A. Bostan, F. Morain, B. Salvy, É. Schost.

Fast algorithms for computing isogenies between elliptic curves.

Math. Comp. 77, 263, 1755-1778, 2008.



D.X. Charles, K.E. Lauter & E.Z. Goren.

Cryptographic Hash Functions from Expander Graphs.

J. Cryptology 22:93–113, 2009.



J.-M. Couveignes.

Computing ℓ -isogenies with the p -torsion.

Lecture Notes in Computer Science vol. 1122, pages 59–65, Springer-Verlag, 1996.



J.-M. Couveignes.

Isomorphisms between Artin-Schreier tower.

Math. Comp. 69(232): 1625–1631, 2000.



L. De Feo.

Calcul d'isogénies.

Master thesis. <http://www.lix.polytechnique.fr/Labo/Luca.De-Feo/>

Bibliography



L. De Feo & É. Schost.

Fast arithmetics in Artin-Schreier towers over finite fields.
Preprint, 2009.



R.P. Gallant, R.J. Lambert & S.A. Vanstone.

Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms.
CRYPTO '01, LNCS, pages 190–200, Springer, 2001.



P. Gaudry, F. Hess, N. P. Smart.

Constructive and destructive facets of Weil descent on elliptic curves.
J. Cryptology 15:19-46, 2002.



D. Jao, S.D. Miller & R. Venkatesan,

Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?
ASIACRYPT '05, LNCS, pages 21–40, Springer, 2005.

Bibliography



A. Joux, R. Lercier.

Counting points on elliptic curves in medium characteristic.
Cryptology ePrint Archive 2006/176, 2006.



R. Lercier, T. Sirvent.

On Elkies subgroups of ℓ -torsion points in curves defined over a finite field.
To appear *J. de Théorie des Nombres de Bordeaux*.



R. Schoof.

Counting points on elliptic curves over finite fields.
J. de Théorie des Nombres de Bordeaux, 7:219-254, 1995.



B. Smith.

Isogenies and the Discrete Logarithm Problem in Jacobians of genus 3 hyperelliptic curves.
In *EUROCRYPT '08*, LNCS, Springer, 2008.



E. Teske.

Elliptic curve trapdoor system.
J. Cryptology 19:115-133, 2006.