Computing isogenies in small or medium characteristic

A.Joux R. Lercier

Université de Versailles — DGA — France

Antoine.Joux (at) m4x.org
Reynald.Lercier (at) m4x.org

Workshop on "Curves, isogenies and cryptologic applications"

Motivation

The quest for efficient algorithms to perform computations in finite fields $\mathbb{F}_{p^n}$ (i.e. asymptotically fast as a function of $\log q$, $q = p^n$), is (too) often restricted to the two cases :

- n fixed and p tends to the infinity ($\mathbb{F}_p$ is typical) or
- p fixed and n tends to the infinity ($\mathbb{F}_{2^n}$ is typical).

Hence, until now, not that much people designed algorithms with reasonable behaviors when n and p both tend to ∞.

But, recently, new algorithms for computing discrete logarithms in $\mathbb{F}_{p^n}$ [JL06, JLSV06] yield surprisingly low complexities in this setting...

How about counting points on elliptic curves ?

Introduction

Let p be a prime, $\mathbb{F}_q$ a finite field with $q = p^n$ elements, E be an elliptic curve defined over $\mathbb{F}_q$. Let P be a point in $E(\overline{\mathbb{F}}_q)$ and denote with ϕ_q the Frobenius endomorphism, then $\phi_q(P) = P$ if and only if P is $\mathbb{F}_q$-rational.

How to efficiently compute $\#E(\mathbb{F}_q)$?

Thanks to Schoof, an algorithm with polynomial time complexity is known whatever the way p and n tend to ∞ [Schoof85, Schoof95].

Weil's dream

The general strategy is based on ideas introduced by Weil, Serre, Grothendieck, Dwork, . . . in order to prove the Weil conjectures.

The dream of Weil was to construct a good cohomology theory such that the number of fixed points of ϕ_q is given by a Lefschetz fixed point formula known in the complex setting as

$$\#\{P \in M \mid f(P) = P\} = \sum_i (-1)^i \operatorname{Tr}(f_* | H^i_{DR}(M)) .$$

(M be a compact complex analytic manifold, $f : M \to M$ an analytic map, f only has isolated non-degenerate fixed points, the $H^i_{DR}(M)$ are called the de Rham cohomology groups of M and are finite dimensional vector spaces over $\mathbb{C}$ on which f induces a linear map f^*)

Grothendieck's breakthrough

Very briefly. . . very restricted the elliptic curve case. . .

Let $\ell \neq p$ and let $\mathbb{Q}_\ell$ be the field of ℓ-adic numbers. Grothendieck introduced the ℓ-adic cohomology groups $H^i(E, \mathbb{Q}_\ell)$ s.t.

$$\#E(\mathbb{F}_q) = \sum_{i=0}^{2} (-1)^i \operatorname{Tr}(\phi_q^*; H^i(E, \mathbb{Q}_\ell)) .$$

The ℓ-adic cohomology groups $H^i(E, \mathbb{Q}_\ell)$ are finite dimensional vector spaces over $\mathbb{Q}_\ell$, which are non-trivial only for $i = 1$,

$$H^1(E, \mathbb{Q}_\ell) \cong T_\ell(E) .$$

Schoof's algorithm

Let $\ell \neq p$ be a prime, let $\chi_E(\phi_q)$ is the characteristic polynomial of ϕ_q on the Tate module $T_\ell(E)$. The main idea is to approximate $T_\ell(E)$ by the ℓ-torsion points $E[\ell]$.

The ℓ-torsion is a 2 dimensional $\mathbb{Z}/\ell\mathbb{Z}$ vector space, and the restriction of ϕ_q to $E[\ell]$ is linear. Let $P_\ell(T)$ denote the characteristic polynomial of this restriction, then $P_\ell(T) \equiv \chi_E(\phi_q)(T) \pmod{\ell}$.

Only one coefficient a_1 of $\chi_E(\phi_q)$ is needed and we have $|a_1| \leq q^{1/2}$ (Riemann hypothesis). Using the Chinese remainder theorem, we can therefore uniquely recover $\chi_E(\phi_q)$ from $P_\ell(T)$ for primes ℓ such that

$$\prod_{\text{primes } \ell, \gcd(\ell,q)=1} \ell > q^{1/2}.$$

This yields a $\widetilde{O}((\log q)^5)$ time complexity (with nothing in n or p hidden in the O) and $O((\log q)^3)$ in space.

Elkies' ideas

For primes ℓ s.t.

- there exists a rational isogeny of degree ℓ defined on E (half the primes),
- the kernel of which can be efficiently computed,

we can compute $P_\ell(T)$ on an (only) 1 dimensional $\mathbb{Z}/\ell\mathbb{Z}$ sub-vector space of $E[\ell]$...

...and we can hope a $\widetilde{O}((\log q)^4)$ time complexity.

Computing isogenies

There exists two classes of algorithms following the characteristic p.

- If $p > \ell$, first algorithms by Elkies, Charlap-Coley-Robbins, the best algorithms [BoMoSaSc06] have $\widetilde{O}((\ell \log q))$ time complexity.
- If $p < \ell$, the previous method yields obstructions. But, when p is fixed, we may consider three other algorithms, mainly :
  - [Couveignes94]. Time $\widetilde{O}(\ell^3 \log q)$, space $O(\ell^2 \log q)$.
  - [Couveignes96]. Time $\widetilde{O}(n\ell \log q)$, space $O(\ell^2 \log q)$.
  - [Lercier96]. For $p = 2$, heuristic time $O(n\ell^3)$, space $O(n\ell^2)$, more efficient for practical use.

Computing isogenies for $\ell \simeq p$

In the worst point counting situation, that is $p \simeq n(\simeq \log q \to \infty)$, one has to compute isogenies of degree $\ell \simeq p$.
[Lercier96] or [BoMoSaSc06] are not an option. It remains Couveignes algorithms but a careful look at their complexities reveal that we have bad powers of p "hidden" in the O constant.

For instance, in [Couveignes96],

- the complexity is at least the cost of computing an isomorphism between two Artin-Schreier extensions defined over $\mathbb{F}_q$,
- if we precompute the inverse of a $pn \times pn$ $\mathbb{F}_p$-matrix,
- then, each isogeny kernel computation involves a matrix-vector multiplication by such a matrix, that is $O((pn)^2)$ bit operations.

SEA algorithm runs thus in $\widetilde{O}(\log^5 q)$ bit operations ...again...

Canonical lift

At the end of 1999, Satoh introduced the p-adic approach to compute the number of points on an ordinary elliptic curve over a finite field [Satoh00].

Let $\overline{\mathcal{A}}$ be an abelian variety defined over $\mathbb{F}_q$ with $q = p^n$. Let $\mathbb{Q}_q$ be an unramified extension of $\mathbb{Q}_p$ of degree n with valuation ring $\mathbb{Z}_q$ and residue field $\mathbb{Z}_q/(p\mathbb{Z}_q) \simeq \mathbb{F}_q$. Consider a lift $\mathcal{A}$ of $\overline{\mathcal{A}}$ defined over $\mathbb{Z}_q$, then in general there exists none $\mathcal{F} \in \mathrm{End}(\mathcal{A})$ that reduces to the Frobenius $\phi_q \in \mathrm{End}(\overline{\mathcal{A}})$.

A canonical lift of an abelian variety $\overline{\mathcal{A}}$ over $\mathbb{F}_q$ is an abelian variety $\mathcal{A}$ over $\mathbb{Z}_q$ such that $\mathcal{A}$ reduces to $\overline{\mathcal{A}}$ modulo p and the ring homomorphism $\mathrm{End}(\mathcal{A}) \longrightarrow \mathrm{End}(\overline{\mathcal{A}})$ induced by reduction modulo p is an isomorphism.

Lubin–Serre-Tate Canonical lift

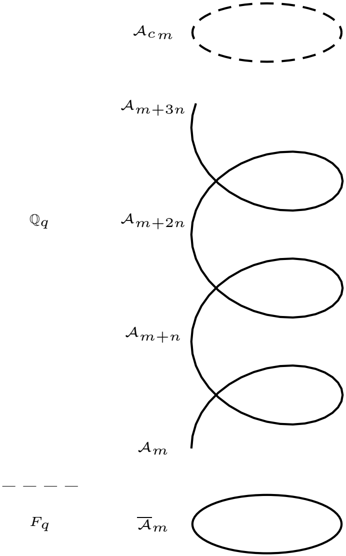
Theorem (Lubin–Serre-Tate) : Let $\overline{A}$ be an ordinary abelian variety over $\mathbb{F}_q$ (i.e. $\overline{\mathcal{A}}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{\dim(\overline{\mathcal{A}})}$). Then there exists a canonical lift $\mathcal{A}_c$ of $\overline{A}$ over $\mathbb{Z}_q$ and $\mathcal{A}_c$ is unique up to isomorphism.

The construction of a p-adic approximation of $\mathcal{A}_c$ given $\overline{\mathcal{A}}$ is as follows:

- Let $\mathcal{A}_0$ be a lift of $\overline{A}$ to $\mathbb{Z}_q$ and $\mathcal{A}_0[p]^{\mathrm{loc}} = \mathcal{A}_0[p] \cap \mathrm{Ker}(\pi_1)$ be the p-torsion points on $\mathcal{A}_0$ that reduce to the neutral element of $\overline{\mathcal{A}}$.
- Then, $\mathcal{A}_1 = \mathcal{A}_0/\mathcal{A}_0[p]^{\mathrm{loc}}$ is again an abelian variety s.t. its reduction is ordinary and there exists an isogeny $I_0 : \mathcal{A}_0 \longrightarrow \mathcal{A}_1$ which reduces to the small Frobenius morphism $\sigma : \overline{\mathcal{A}} \longrightarrow \overline{\mathcal{A}}^{\sigma}$.
- Repeating this construction, we get a sequence of abelian varieties and isogenies $\mathcal{A}_0 \xrightarrow{I_0} \mathcal{A}_1 \xrightarrow{I_1} \dots$.

Clearly $\mathcal{A}_{kn}$ reduces to $\overline{\mathcal{A}}$ modulo p; furthermore, $\{\mathcal{A}_{kn}\}_{k\in\mathbb{N}}$ converges to the canonical lift $\mathcal{A}_c$ and the convergence is linear.

Riemann iterations



p fixed, $O(n^3)$ time complexity

Algorithm `AGM` [Mestre01]

Algorithm to compute the trace of an ordinary elliptic curve $E/\mathbb{F}_{2^n} : y^2 + xy = x^3 + \alpha$.

INPUT: $\alpha \in \mathbb{F}_{2^n}$.
OUTPUT: The trace c of E.

Lift phase

1. $a := 1 + 8\alpha \in \mathbb{Z}_q; b := 1 \in \mathbb{Z}_q;$
2. **for** $(i := 1; i < n/2 + O(1); i := i + 1)$ {
3. $\quad a, b := \frac{a+b}{2}, \sqrt{ab}$;
4. }

Norm phase

5. A := a; B := b;
6. **for** $(i := 1; i < n; i := i + 1)$ {
7. $\quad a, b := \frac{a+b}{2}, \sqrt{ab}$;
8. }
9. **return** $\frac{A}{a}$ mod 2^n as a signed integer in $[-2\sqrt{2^n}, 2\sqrt{2^n}]$.

$O(n^2)$ time complexity, but...

Thanks to numerous people in this field, when p id fixed, $O(n^2)$ time complexity can be achieved.

For non fixed p... one bottleneck is that we can not avoid the calculation of the p-torsion part of the curve and this involves the computation in the p-adics of the p-th division polynomial.

The best algorithms run finally in $\widetilde{O}(p^2 n^2)$ bit operations, but requires a $O(p^2 n^2)$ memory.

One may think to Kedlaya's algorithm in this setting, but again the complexity, both in time and space, is reported to be $\widetilde{O}(pn^3)$.

$\widetilde{O}(\log^4 q)$ bit operations, but a (too large) $O(\log^4 q)$ in storage too.

The idea

In our worst point counting case, $p \simeq n (\simeq \log q \to \infty)$, we would like to get rid of the obstructions which arise with isogeny algorithms for $\ell > p$.

In the same spirit as for counting points in the Satoh-Mestre like fashion, we propose to lift the isogeneous elliptic curves in an unramified extension denoted $\mathbb{Q}_q$ of the p-adic (corresponding to the extension $\mathbb{F}_q$ of $\mathbb{F}_p$).

So that the inversions by p which may occur in the isogeny algorithms are no longer a problem (at least for computations with with enough precision).

Algorithm `IsogenyLifted` [JL06a]

Algorithm to compute separable kernels of isogenies of degree ℓ

INPUT: An non-supersingular elliptic curve given over $\mathbb{F}_q$ by $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_x + a_6$ and an Elkies prime ℓ.
OUTPUT: Two polynomials in $\mathbb{F}_q[X]$ of degree $\lfloor \ell/2 \rfloor$ the roots of which are x-coordinates of points of $E[\ell]$.

1. Let $w = O(\ell/p)$ be a p-adic precision.

2. Lift E in $\mathbb{Q}_q$ in a arbitrary way.

3. Compute an isomorphic Weierstraß model $\mathcal{E} : y^2 = x^3 + A_4x + A_6$ isomorphic by λ to $E/\mathbb{Q}_q$.

4. Use Atkin-Elkies' algorithm to get at precision w in $\mathbb{Q}_q$ two isogeneous curves $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{E}}'$.

5. Use Atkin-Elkies' algorithm to get at precision w in $\mathbb{Q}_q$ the sums p_1 and p_1'.

6. Take the isogeny algorithm of your choice to get from $(\tilde{\mathcal{E}}, p_1)$ and $(\tilde{\mathcal{E}}', p_1')$ two polynomials $\mathcal{H}_\ell(X)$ and $\mathcal{H}_\ell'(X)$.

7. **return** $\{\lambda^{-1}(\mathcal{H}_\ell(X)) \bmod p,\ \lambda^{-1}(\mathcal{H}'_\ell(X)) \bmod p\}$.

Complexity analysis

We studied the Charlap-Coley-Robbins algorithm in this case.

Mainly :

- the precision needed depends on the number of non invertible elements that the algorithm will encounter, that is

$$\lfloor 15 + 3\ell/2 \rfloor \text{ if } p = 2, 5 + \ell \text{ if } p = 3 \text{ and } \lfloor 1 + 2\ell/p \rfloor \text{ otherwise.}$$

- the complexity in time of the algorithm is still $\widetilde{O}(\ell^2)$ multiplications... but in $\mathbb{Q}_q$, at precision $\widetilde{O}(\ell/p)$. We therefore have a total complexity in time equal to $\widetilde{O}((1 + \ell/p)\ell^2 \log q)$. The complexity in space is $O((1 + \ell/p)\ell \log q)$.

Example, a degree 13 isogeny in $\mathbb{F}_{23}$

Let $E/\mathbb{F}_{23}\ : y^2 = x^3 + 6\,x + 17.$ We take as Weierstraß model isomorphic to E in $\mathbb{Q}_{23}$ at precision 2 the curve

$$\mathcal{E} : y^2 = x^3 + (6 + O(23^2))\,x + (17 + O(23^2)).$$

Atkin-Elkies' algrithms then enable us to find that $\mathcal{E}$ is 13-isogeneous to a curve approximated by $\tilde{\mathcal{E}} : y^2 = x^3 + (99 + O(23^2))\,x$.
Charlap-Coley-Robbins algorithm applied to these inputs yields

$$\begin{aligned}\mathcal{H}_{23}(X) = X^6 + (19 + O(23^2))\,X^5 - (50 + O(23^2))\,X^4 + (208 + O(23^2))\,X^3 \\ - (119 + O(23^2))\,X^2 - (252 + O(23^2))\,X - 231 + O(23^2).\end{aligned}$$

Reducing the result modulo 23, we finally find that

$$h_{23}(X) = X^6 + 19\,X^5 + 19\,X^4 + X^3 + 19\,X^2 + X + 22.$$

Conclusion

In our main concern, $p \simeq n \simeq \log q$, plugging this isogeny algorithm in the SEA framework yields, for the first time, a nice $\widetilde{O}(\log^4 q)$ complexity in time, and a at most $\widetilde{O}(\log^3 q)$ complexity in space.

With a more efficient isogeny algorithm, as the one of [BoMoSaSc06], we *might expect* to reduce the isogeny complexity phase as low as $\widetilde{O}((1 + \ell/p)\ell \log q)$, but we may not have such a low complexity for the overall computation, due to the computation of the isogenous curves in $\mathbb{Q}_q$, via modular polynomials.

Bibliography I

A. Bostan, F. Morain, B. Salvy and É. Schost
Fast algorithms for computing isogenies between elliptic curves
Preprint

J.-M. Couveignes.
Quelques calculs en théorie des nombres.
thèse, Université de Bordeaux I, July 1994.

J.-M. Couveignes.
Computing l-isogenies with the p-torsion.
In H. Cohen, editor, *ANTS-II*, volume 1122 of *Lecture Notes in Computer Science*, pages 59–65. Springer-Verlag, 1996.

A. Joux and R. Lercier.
The Function Field Sieve in the Medium Prime case.
Eurocrypt 2006.

A. Joux and R. Lercier.
Counting points on elliptic curvs in medium characteristic.
Cryptology eprint archive, report 2006/176.

A. Joux, R. Lercier, N. Smart, and F. Vercauteren.
The Number Field Sieve in the Medium Prime case.
Crypto 2006.

Bibliography II

R. Lercier.
Computing isogenies in $\mathbf{F}_{2^n}$.
In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Computer Science*, pages 197–212. Springer, Berlin, 1996.

J.-F. Mestre.
AGM pour le genre 1 et 2, 2001.
Lettre à Gaudry et Harley. Available at *http://www.math.jussieu.fr/~mestre*.

T. Satoh.
The canonical lift of an ordinary elliptic curve over a finite field and its point counting.
J. Ramanujan Math. Soc., 15(4):247–270, 2000.

R. Schoof.
Elliptic curves over finite fields and the computation of square roots mod p.
Mathematics of Computation, 44:483–494, 1985.

R. Schoof.
Counting points on elliptic curves over finite fields.
Journal de Theorie des nombres de Bordeaux, 7:219–254, 1995.
Available at *http://www.emath.fr/Maths/Jtnb/jtnb1995-1.html*.