

# Towards computing canonical lifts of ordinary elliptic curves in medium characteristic

ABDOULAYE MAIGA AND DAMIEN ROBERT

ABSTRACT. Let  $p$  be a prime; using the dimensional one modular polynomial  $\Phi_p$ , T.Satoh and al [Sat00b; R; Ver03] developed several algorithms to compute the canonical lift of an ordinary elliptic curve  $E$  over  $\mathbb{F}_{p^n}$  with  $j$ -invariant not in  $\mathbb{F}_{p^2}$ . When  $p$  is constant, the best variant has a complexity  $\tilde{O}(nm)$  to lift  $E$  to  $p$ -adic precision  $m$ . As an application, lifting  $E$  to precision  $m = O(n)$  allows to recover its cardinality in time  $\tilde{O}(n^2)$ . However, taking  $p$  into account the complexity is  $\tilde{O}(p^2nm)$ , so Satoh's algorithm can only be applied to small  $p$ .

We propose in this paper two variants of these algorithms, which do not rely on the modular polynomial, for computing the canonical lift of an ordinary curve. Our new method yield a complexity of  $\tilde{O}(pnm)$  to lift at precision  $m$ , and even  $\tilde{O}(\sqrt{pnm})$  when we are provided a rational point of  $p$ -torsion on the curve. This allows to extend Satoh's point counting algorithm to larger  $p$ .

**Key words:** Canonical lift of Elliptic curves, Isogeny computation, Point counting.

## 1. INTRODUCTION

Let  $E/\mathbb{F}_q$  be an elliptic curve over a finite field. Schoof's algorithm [Sch85] give a polynomial time algorithm to count the number of point of  $E$ . The complexity was later improved by Atkin and Elkies to give the SEA algorithm [Elk92; Elk98; BMS+08]. The algorithm can be seen as an incarnation of  $\ell$ -adic étale cohomology: if  $\chi(t)$  is the characteristic polynomial of the Frobenius  $\pi_q$ ,  $\chi(t) \bmod \ell$  is computed modulo several primes  $\ell$  by looking at the action of  $\pi_q$  on (a subgroup of) the  $\ell$ -torsion  $E[\ell]$ . The CRT algorithm allows to reconstruct  $\chi(t)$  once we have enough precision (as bounded by the Hasse-Weil bound). One can compute  $\chi \bmod \ell$  in  $\tilde{O}((\ell + \log q)\ell \log q)$ , hence reconstruct  $\chi$  in  $\tilde{O}(\log^4 q)$ .

In 2000, a second class of algorithms was introduced by Satoh [Sat00a], using the Lubin-Serre-Tate Theorem. Let  $q = p^n$ , let  $\mathbb{Z}_q$  denotes the ring of Witt vectors of  $\mathbb{F}_q$ , and  $\mathbb{Q}_q = \text{Frac}(\mathbb{Z}_q)$  the unique unramified extension of  $\mathbb{Q}_p$  of degree  $n$ . Then [LST64a] establishes the existence of a unique (up to isomorphisms) elliptic curve  $\tilde{E}$  over  $\mathbb{Z}_q$  for every ordinary elliptic curves  $E/\mathbb{F}_q$  such that the modulo  $p$  reduction of  $\tilde{E}$  is  $E$  and  $\text{End}(\tilde{E}) \cong \text{End}(E)$  as a ring. The curve  $\tilde{E}$  is called the *canonical lift of  $E$* . Then the trace of the Frobenius morphism is deduced using *crystalline cohomology*. After improvements by Harley, Satoh's algorithm can compute the canonical lift to precision  $m$  in quasi-linear time  $\tilde{O}_p(nm)$ . Here the notation  $\tilde{O}_p$  means that we assume that  $p$  is a constant. We can then recover the inversible eigenvalue of the Frobenius at precision  $m$  in the same time. By Hasse's bound, it suffices to work at precision  $m = O(n)$  to recover the full eigenvalue, so Satoh's algorithm gives a point counting algorithm of quasi quadratic complexity  $\tilde{O}_p(n^2)$ .

---

Date: March 16, 2022.

Key words and phrases. canonical lift, point counting.

We thank the FAST team and CIAO ANR Project.

We are interested in the dependency of  $p$  of the algorithm. We will now assume that  $p > 2$  for simplicity. For an ordinary elliptic curve  $E/\mathbb{F}_q$ , Satoh's algorithm and its improvements [Ver03; R] proceeds in four steps:

- (1) Compute the canonical lift  $\tilde{E}/\mathbb{Z}_q$  at  $p$ -adic precision  $m$  by solving the equation  $\Phi_p(j(\tilde{E}), \Sigma(j(\tilde{E}))) = 0$  via a Newton lift. Here  $j$  is the  $j$ -invariant,  $\Phi_p$  the modular polynomial classifying  $p$ -isogenies, and  $\Sigma$  the (small) Frobenius on  $\mathbb{Z}_q$ .
- (2) Lift the kernel  $E[p]_{\text{et}}$  of the Verschiebung to  $\tilde{E}$  via a Newton lift. The kernel of the Verschiebung modulo  $p$  is defined by the  $x$ -coordinates of its points:  $H_p(x) = \prod_{P \in E[p]_{\text{et}} \setminus \{0_E\}} (x - x(P))$ , and its lift  $\tilde{H}_p$  is the unique étale lift dividing the  $p$ -division polynomial  $\Psi_p(\tilde{E})$ .
- (3) Compute the isogeny  $\tilde{E} \rightarrow \tilde{E}/\tilde{H}_p$  using Vélu's formula, and an isomorphism  $u$  between  $\tilde{E}/\tilde{H}$  and  $\hat{\Sigma}(\tilde{E})$ . Since Vélu's isogenies are normalised, applying  $\Sigma$  to this isomorphism  $u$  gives (up to a sign) the action  $\lambda_0$  of  $\tilde{\pi}$  on the tangent spaces  $dx/y$  and  $\Sigma(dx/y)$  of  $\tilde{E}$  and  $\tilde{E}^\sigma$ .
- (4) Compute the norm  $\lambda = N_{\mathbb{Q}_q/\mathbb{F}_q}(\lambda_0)$ . This recovers the invertible eigenvalue of the big Frobenius  $\pi_q$  at precision  $m$ , up to a sign. The correct sign is chosen using Hasse's invariant. The trace is then given by  $t = \lambda + q/\lambda$ , and if  $m \geq (n+5)/2$ , the value of  $t$  at  $p$ -adic precision  $m$  is enough to recover  $t$  in  $\mathbb{Z}$ . Then  $\chi_\pi(x) = x^2 - tx + q$ .

The modular polynomial  $\Phi_p(X, Y)$  is of total degree  $p+1$  and its logarithm height is  $h(\Phi_p) \leq 6p \log p + 18p$  (see [BS09]). Thus its total size is of  $\tilde{O}(p^3)$ , and there are quasi-linear algorithms to compute it [Eng09]. Step 1 is done via Newton iterations, the dominating step is evaluating  $\Phi_p$  at precision  $m$  in  $\mathbb{Z}_q$ , for a cost of  $\tilde{O}(p^2 m \log q) = \tilde{O}(p^2 mn)$ . Step 2 is also done via Newton iterations, the dominating step is evaluating the division polynomial  $\Psi_p(X)$ , which is of degree  $(p^2-1)/2$  at precision  $m$ , for a total cost of  $\tilde{O}(p^2 m \log q) = \tilde{O}(p^2 mn)$ . Step 3 is dominated by Vélu's formula and costs  $\tilde{O}(pm \log q) = \tilde{O}(pmn)$ . In Step 4 the norm is done via a resultant, and also costs  $\tilde{O}(pm \log q) = \tilde{O}(pmn)$ . Since  $m = O(n)$ , the final complexity of Satoh's algorithm is thus  $\tilde{O}(p^3 + p^2 m \log q) = \tilde{O}(p^3 + p^2 n^2)$ . By contrast, the SEA algorithm (in particular the version of [LS08] which works in all characteristic) has a complexity of  $\tilde{O}(n^4)$ , so Satoh's algorithm has better complexity for small  $p$  and large  $n$ . We note that the complexity of  $\tilde{O}(p^3)$  comes from the computation of  $\Phi_p(x, y)$ . This polynomial only depends on  $p$ , not on the elliptic curve, so this part may be seen as a precomputation, and the real complexity of Satoh's algorithm is  $\tilde{O}(p^2 n^2)$ . Alternatively one could use the techniques of [Rob21a, § 5.3.8] to evaluate  $\Phi_p$  directly.

In 2002, given an affine equation  $f(x, y) = 0$  of  $E$ , Kedlaya proposed in [Ked01a] to use the Monsky-Washnitzer cohomology associated to  $A^\dagger = \mathbb{Q}_q \langle \langle x, y \rangle \rangle / \tilde{f}(x, y)$ . The difference between these two  $p$ -adic methods is the unicity of the canonical lift in Satoh's method in contrast to Kedlaya's method where the lift is arbitrary. Kedlaya's approach [Ked01b] thus computes a non-specific lift with linear complexity in  $p$  and then reconstructs  $\chi$  with complexity in time (and space) of  $O_p(n^{3+\epsilon})$ . Harvey in [Har07] improved the dependency on  $p$  of Kedlaya's algorithm. More precisely he shows that Kedlaya's original algorithm can compute the Frobenius to  $p$ -adic precision  $m$  with a complexity of  $\tilde{O}(pn^2 m)$ , and Harvey improves the dependency on  $p$  to  $\tilde{O}(\sqrt{pn}^{5/2} m + n^4 m \log p)$  (at the cost of a worse dependency on  $m$ ).

It is such natural to ask whether there exists an algorithm that has the  $\tilde{O}_p(nm)$  quasi-linear complexity of Satoh's algorithm with respect to  $n$  and the precision  $m$  but improves the  $\tilde{O}(p^2)$  dependency on  $p$  (which is even  $\tilde{O}(p^3)$  if we take into account the precomputation of the modular polynomial when we don't use the direct evaluation strategy of [Rob21a]) to Harvey's  $\tilde{O}(\sqrt{p})$ .

Isogeny based key exchange protocols rekindled the interest of the second author on computing canonical lifts to high precision  $m$ . (We stress that so far we are not aware of applications

other than point counting, which only require a precision  $m = O(n)$ .) He proposed in [Rob21b, Chapter 6] a new approach of Satoh's method which works by only using the modular polynomial  $\Phi_p$  to both lift the curve and the isogeny. This allows to dispense with the computation of the division polynomial  $\Psi_p$ , but does not change the asymptotic because of the evaluation of the modular polynomial, so the algorithm is still in  $\tilde{O}(p^3 + p^2 nm \log p)$  (although with better constants).

He proposed another method bypassing the need for the modular polynomial in [Rob21b, Remark 6.6.2], assuming a point of  $p$ -torsion is given on  $E$ . More recently, he realized that by working modulo  $H_p$  directly allows to define a "formal" point of  $p$ -torsion to which to apply [Rob21b, Remark 6.6.2]. This allows to bypass the need to find a point of  $p$ -torsion. These two strategies (working with a rational point of  $E_{\text{et}}[p]$  or with its formal point defined by  $H_p$ ) were implemented in Pari/GP by the first author, who also carefully tracked the loss of precision. The implementation showed that the resulting algorithms not only improve the theoretical complexity but are also practical. This is the subject of the present work.

Indeed, we can keep the  $\tilde{O}_p(nm)$  complexity of Satoh's algorithm while improving the dependency on  $p$ .

**Theorem 1.1.** *Let  $E/\mathbb{F}_q$  be an ordinary elliptic curve, with  $j(E) \notin \mathbb{F}_{p^2}$ . Then one can compute the canonical lift  $\tilde{E}/\mathbb{Z}_q$  and the trace of the Frobenius to  $p$ -adic precision  $m$  in time  $\tilde{O}(mnp)$ .*

*In particular, for point counting where we need  $m = O(n)$ , the complexity to compute  $\chi_\pi$  is  $\tilde{O}(pn^2)$ .*

The main idea behind Theorem 1.1, is that when doing a Newton lift to lift the root of a polynomial  $F(X)$ , it is not necessary to be given  $F$ , one only needs to be able to evaluate it. We can thus circumvent computing the modular polynomial  $\Phi_p$  and the division polynomial  $\Psi_p$  in Satoh's algorithm by directly evaluating isogenies (ie solving the equation  $j(E^\nu) = j(E^{\hat{\Sigma}})$  where  $E^\nu$  is computed via an isogeny) and the multiplication by  $[p]$  map.

Although we do not reach Harvey's  $\tilde{O}(\sqrt{p})$  complexity, in some cases a variant of our method achieve such a complexity.

**Theorem 1.2.** *Let  $E/\mathbb{F}_q$  be an ordinary elliptic curve with  $j(E) \notin \mathbb{F}_{p^2}$ , and assume that we are given a rational étale point of  $p$ -torsion  $P$ . Let  $I(d, m, \mathbb{Z}_q)$  be the cost of evaluating at precision  $m$  an isogeny of degree  $d$  on an elliptic curve  $E'$  over  $\mathbb{Z}_q$  given a generator  $P$  (defined over  $\mathbb{Z}_q$ ) of its kernel. Here by evaluating the isogeny, we only mean computing the equations of  $E'/\langle P \rangle$  at precision  $m$ .*

*Then one can compute the canonical lift  $\tilde{E}/\mathbb{Z}_q$  and the trace of the Frobenius to  $p$ -adic precision  $m$  in time  $\tilde{O}(mn \log p + I(p, m, \mathbb{Z}_q))$ .*

**Remark 1.3.** We can also work on the Kummer line  $E/\pm 1$ , that is given only the  $x$ -coordinate  $x_P$  of our point  $P$ , in which case  $I(d, m, \mathbb{Z}_q)$  should be the cost of evaluating the induced isogeny  $E/\pm 1 \mapsto (E/\langle P \rangle)/\pm 1$ .

Using Vélú's formula, we have  $I(p, m, \mathbb{Z}_q) = \tilde{O}(pm \log q) = \tilde{O}(pmn)$ . A recent improvement of Vélú's formula [BDL+20] improves this complexity to  $\tilde{O}(\sqrt{p}m \log q) = \tilde{O}(\sqrt{p}mn)$ .

In general, the étale points of  $p$ -torsion will live in an extension of degree  $e \leq p-1$  (which we can compute using Hasse's formula), and to find one of them require computing a root of the division polynomial  $\Psi_p$  modulo  $p$ , which can be done in time  $\tilde{O}(p^2 \log q + p \log^2 q) = \tilde{O}(np^2 + pn^2)$ . We explain how to improve this complexity to  $\tilde{O}(p \log^2 q)$  in Section 4.2 and get:

**Corollary 1.4.** *Let  $e$  be the degree of the extension of  $\mathbb{F}_q$  where the étale points of  $p$ -torsion lives. Then one can compute the canonical lift  $\tilde{E}/\mathbb{Z}_q$  and the trace of the Frobenius to  $p$ -adic*

precision  $m$  in time  $\tilde{O}(p \log^2 q + \sqrt{p} m e \log q) = \tilde{O}(pn^2 + \sqrt{p} m e n)$ . (If  $\chi_\pi$  is already known the complexity becomes  $\tilde{O}(\log^2(q^e) + \sqrt{p} m e \log q) = \tilde{O}(e^2 n^2 + \sqrt{p} m e n)$ .)

In the worst case,  $e = O(p)$  so the complexity is  $\tilde{O}(p \log^2 p + p^{3/2} m \log q) = \tilde{O}(pn^2 + p^{3/2} m n)$  is not better than Theorem 1.1. In the best cases, when  $e = O(\log p)$ ; for instance if the trace  $t = 1 \pmod p$  (which implies  $e = 1$ ); the complexity is  $\tilde{O}(p \log^2 q + p^{1/2} m \log q) = \tilde{O}(pn^2 + p^{1/2} m n)$ . In general, to compute  $\tilde{E}$  at high  $p$ -adic precision, we improve on the complexity of Theorem 1.1 whenever  $e = O(\sqrt{p})$ .

We organize this paper as follow. In Section 2, we recall the Serre-Tate theorem and Satoh's algorithm. We present our new approach to Newton lifts in Section 3. As a first application we explain how to lift the  $p$ -torsion in Section 4, then we give our canonical lift algorithm in Section 5.

**1.1. Notation and Convention.** In the following  $p$  is prime and  $q = p^n$  with  $n \geq 1$ .

We denote by  $\mathbb{Q}_q$  the unramified extension of the field of  $p$ -adic numbers  $\mathbb{Q}_p$  and by  $\mathbb{Z}_q$  is the valuation ring of  $\mathbb{Q}_q$ ; it is also the ring  $W(\mathbb{F}_q)$  of the Witt vectors over  $\mathbb{F}_q$ . The extension  $\mathbb{Q}_q/\mathbb{Q}_p$  has a cyclic Galois group of order  $n$ , generated by an element  $\Sigma$  that reduces to the (small) Frobenius automorphism  $\sigma$  on the residue field  $\mathbb{F}_q$ . The large Frobenius (and its lift) will be denoted by  $\sigma_q$  and  $\Sigma_q$  respectively, and sometime we will denote  $\sigma$  by  $\sigma_p$  to emphasize we work with the small Frobenius. As a convenience we let  $\hat{\sigma} = \sigma^1 = \sigma^{n-1}$ ,  $\hat{\Sigma} = \Sigma^{n-1}$ , the ‘‘Verschiebung’’ Galois elements.

Explicitly  $\mathbb{Q}_q = \mathbb{Q}_p[X]/M(X)$  and also  $\mathbb{Z}_q = \mathbb{Z}_p[X]/M(X)$  with  $M$  is monic irreducible polynomial of degree  $n$  over  $\mathbb{Z}_p[X]$  with irreducible reduction modulo  $p$ . The complexity of an elementary operation require  $\tilde{O}(m \log q) = \tilde{O}(mn)$  with Kronecker-Schönhage method at precision  $m$ . By  $p$ -adic precision  $m$ , we mean that we are working modulo  $p^m \mathbb{Z}_q$ . Furthermore, fast modular composition [KU11] allows to efficiently evaluate  $\Sigma$  and  $\hat{\Sigma}$  in  $\tilde{O}(nm)$ ; it also allows to evaluate  $\hat{\sigma}$  in  $\tilde{O}(\log q) = \tilde{O}(n)$  rather than the slower  $\tilde{O}(n \log q) = \tilde{O}(n^2)$  we get iterating the Frobenius  $n - 1$  times. It is also convenient to take for  $M$  the Teichmuller lift of an irreducible polynomial  $\bar{M}(X)$  of degree  $n$  over  $\mathbb{F}_p$ , this allows for a fast computation of  $\Sigma$  without invoking modular composition.

We recall the Frobenius  $\sigma_p$  induces an isogeny  $\pi_p : E \rightarrow E^\sigma, P \mapsto P^\sigma$ , and  $\sigma_q$  induces an endomorphism  $\pi_q$ . The Verschiebung  $\hat{\pi} : E \rightarrow E^{\hat{\sigma}}$  is the dual of  $\pi_p : E^{\hat{\sigma}} \rightarrow E$  (we warn that it is not given on points by  $P \mapsto P^{\hat{\sigma}}$ ). Both the Frobenius and Verschiebung lift uniquely to the canonical lifts, we denote them by  $\tilde{\pi}$  and  $\tilde{\hat{\pi}}$ . In this article,  $E^\dagger$  we always denote the canonical lift of  $E$ , while  $\tilde{E}$  will denote a candidate lift (which may or may not be canonical).

## 2. BACKGROUND

Let  $E/\mathbb{k}$  be an elliptic curve, and  $\Psi_\ell$  its polynomial of  $\ell$ -torsion (or  $\ell$ -division polynomial) associated with the equation of the curve. A point  $P = (x, y)$  on  $E$  is a point of  $\ell$ -torsion if and only if its coordinates constitute a solution of  $\Psi_\ell$ .

An isogeny  $\phi$  is a non trivial morphism between elliptic curves which is also a group morphism. The multiplication morphism is identified with  $\mathbb{Z}$  then  $\mathbb{Z} \subset \text{End}(E)$ . Furthermore when the base field  $\mathbb{k}$  is  $\mathbb{F}_q$  we have:  $\mathbb{Z}[\pi_q] \subset \text{End}(E)$  where  $\pi_q$  is the Frobenius endomorphism. In the case where  $E$  is ordinary:  $\chi(X) = X^2 - tX + q$  is the characteristic polynomial of  $\pi_q$  where  $t$  is the trace of  $\pi_q$  and verifies the relation  $|t| \leq 2\sqrt{q}$  called Hasse's bound. Therefore, if we set  $D_{\pi_q} = t^2 - 4q < 0$  then :  $\#E(\mathbb{k}) = q + 1 - t$  and  $\mathbb{Z}[\pi_q] \subset \text{End}(E) \subset \mathcal{O}_{\mathbb{K}}$  where  $\mathbb{K} = \mathbb{Q}[\sqrt{D_{\pi_q}}]$ .

**2.1. Vélú's Algorithm.** According to the inputs, the algorithms for calculating isogenies can be classified into two large groups. The first ones initiated by Vélú [Vél71] takes an elliptic curve  $E$

and a subgroup  $K$  of  $E$  then outputs an explicit form of isogeny  $\phi : E \rightarrow E/K$  and an equation of  $E/K$ . Then for every  $P \in E$ :

$$x_{\phi(P)} = x_P + \sum_{Q \in K^*} (x_{P+Q} - x_Q) \quad \text{and} \quad y_{\phi(P)} = y_P + \sum_{Q \in K^*} (y_{P+Q} - y_Q).$$

Considering the improvements made by D. Kohel [Koh96] we arrive at the same results when  $K = \ker \phi$  is represented by a polynomial  $h$ .

**Example 2.1.** When  $\text{char}(\mathbb{k}) \geq 3$  and an elliptic curve  $E$  over  $\mathbb{k}$  is given by  $E : y^2 = f(x) = x^3 + a_4x + a_6$ .

Let  $h$  be the polynomial defines the kernel  $K$  of a separable normalised isogeny  $\phi$  of degree  $\ell$  with domain  $E$  Set:

$$\begin{aligned} Q(x) &= \gcd(f(x), h(x)) \\ D(x) &= h(x)^2/Q(x) \\ &= x^{\ell-1} - d_1x^{\ell-2} + d_2x^{\ell-3} - d_3x^{\ell-4} + \dots \end{aligned}$$

Then for every point  $P(x, y)$  in  $E$  we have:

$$\begin{aligned} \phi(x, y) &= (\alpha(x), y\alpha(x)) \\ \text{where } \alpha(x) &= \ell x - d_1x - (3x^2 + a_4) \cdot \frac{D'(x)}{D(x)} - 2f(x) \cdot \left( \frac{D'(x)}{D(x)} \right)'. \end{aligned}$$

And  $E/K$  is given by the equation:

$$y^2 = x^3 + (a_4 - 5v)x + (a_6 - 7w)$$

$$\text{where } v = a_4(\ell - 1) + 3(d_1^2 - 2d_2) \quad \text{and} \quad w = 3a_4d_1 + 2a_6(\ell - 1) + 5(d_1^3 - 3d_1d_2 + 3d_3).$$

On the other hand, the modular polynomial  $\phi_p$  encodes directly the  $j$ -invariants of isogeneous elliptic curves.

## 2.2. Lubin Serre Tate theory.

**Theorem 2.2.** (Lubin-Serre-Tate) Consider  $E$  an ordinary elliptic curve over  $\mathbb{F}_q$ , then there exist a unique elliptic curve up to isomorphism  $\tilde{E}$  over  $\mathbb{Z}_q$  such that.

- $E$  is the reduction of  $\tilde{E}$  modulo  $p$ ,
- $\text{End}(\tilde{E}) \cong \text{End}(E)$ ,

$\tilde{E}$  is called the canonical lift of  $E$ , and is also uniquely characterised by the fact that the Frobenius  $\pi_q$  lift to  $\tilde{E}$ , or that  $\pi_p$  lift to an isogeny  $\tilde{E} \rightarrow \tilde{E}^\Sigma$ , ie by the equation

$$\Phi_p(j(\tilde{E}), j(\tilde{E}^\Sigma)) = 0.$$

$$\begin{array}{ccc} \tilde{E} & \xrightarrow{\tilde{\pi}} & \tilde{E}^\Sigma \\ \downarrow & & \downarrow \\ E & \xrightarrow{\pi} & E^\sigma \end{array}$$

We refer to [LST64b] for the statements (without proofs) and [Mes72] for proofs.

**Remark 2.3.** If  $\tilde{E}/\mathbb{Z}_q$  is an elliptic curve, then it is the Néron model of its generic fiber  $\tilde{E}_\eta$ . Furthermore, by the property of Néron models,  $\tilde{E}(\mathbb{Z}_q) = \tilde{E}_\eta(\mathbb{Q}_q)$ . Hence it is harmless to consider the curve over  $\mathbb{Q}_q$ .

**2.3. Modular Equations.** We present Satoh's (as improved by Harley) method to compute the canonical lift  $\tilde{E}$  using the modular relation  $\Phi_p(j(\tilde{E}), j(\tilde{E})^\Sigma) = 0$ .

We know that the modular polynomial satisfy the Kronecker's relation:

$$\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod{p}$$

Let  $j \notin \mathbb{F}_{p^2}$ , the following statement is an immediate consequence of *Kronecker's relation*:

$$\begin{cases} \frac{\partial \Phi_p}{\partial X}(j, j^\sigma) \equiv j^p - j^p \equiv 0 \pmod{p} \\ \frac{\partial \Phi_p}{\partial Y}(j, j^\sigma) \equiv j^{p^2} - j \not\equiv 0 \pmod{p} \end{cases}$$

Thus we deduce that the Frobenius  $\sigma$  has multiplicity 1 and the Verschiebung  $\hat{\sigma}$  has multiplicity  $p$ . In fact we have over  $\mathbb{Q}_q$  two points  $(P, Q)$  on  $\tilde{E}[p]$  that reduce to  $\bar{P}$  and 0 respectively. The  $p$  kernels  $\langle P + kQ \rangle$  with  $0 \leq k < p$  reduce to  $\bar{P}$  (ie the kernel of the Verschiebung) and the last  $\langle Q \rangle$  reduces to  $\langle \mathcal{O} \rangle$  (ie the kernel of the Frobenius). So we have  $p$ -isogenies on  $\tilde{E}$  which reduces to the Verschiebung  $\hat{\pi}$  modulo  $p$ . A more detailed analysis show that they reduce to different isogenies modulo  $p^2$ , hence:

**Lemma 2.4.** *Let  $\tilde{E}/\mathbb{Z}_q$  be any lift of  $E/\mathbb{F}_q$  where  $j(E) \notin \mathbb{F}_{p^2}$ . Then  $\frac{\partial \Phi_p}{\partial X}(j(\tilde{E}), j(\tilde{E})^\sigma)$  is of valuation 1.*

*Proof.* By [Nak93, Proposition 2], since  $j(\tilde{E}) \neq 0, 1728$ ,  $\Phi_p(j(\tilde{E}), X) = (X - j(\tilde{E})^\Sigma)(X - j(\tilde{E})^{\hat{\Sigma}})G(X)$  where  $G(X + j(\tilde{E})^{\hat{\Sigma}})$  is an Eisenstein polynomial. Since  $j(\tilde{E}) \notin \mathbb{F}_{p^2}$ ,  $j(\tilde{E})^\Sigma \neq j(\tilde{E})^{\hat{\Sigma}}$  and the result follows.  $\square$

This provides an algorithm to compute the lifted  $j$ -invariants of the  $p$ -isogenous curves  $\tilde{E}$  and  $\tilde{E}^\Sigma$ .

We want to solve in  $\mathbb{Z}_q$  the equation  $\Phi_p(\tilde{j}, \tilde{j}^\sigma) = 0$  knowing  $\tilde{j}$  modulo  $p$ . Suppose that we can compute efficiently the Frobenius  $\Sigma$  of  $\mathbb{Q}_q$  and  $x \in \mathbb{Z}_q$  is an approximation of  $\tilde{j}$  at precision  $k$  i.e  $\tilde{j} = x + p^k e$  for some error  $e \in \mathbb{Z}_q$  that we want to find. Using the modular equation and Taylor expansion of  $\Phi_p$  we have:

$$\begin{aligned} 0 &= \Phi_p(x + p^k e, x^\sigma + p^k e^\sigma) \\ 0 &= \Phi_p(x, x^\sigma) + p^k e \frac{\partial \Phi_p}{\partial X}(x, x^\sigma) + p^k e^\sigma \frac{\partial \Phi_p}{\partial Y}(x, x^\sigma) + p^{2k}(\dots) \end{aligned}$$

Dividing by  $p^k$ , we get

$$u + e \frac{\partial \Phi_p}{\partial X}(x, x^\sigma) + e^\sigma \frac{\partial \Phi_p}{\partial Y}(x, x^\sigma) \equiv 0 \pmod{p^k}.$$

If  $j \notin \mathbb{F}_{p^2}$ , the Kronecker inequality implies that  $\frac{\partial \Phi_p}{\partial X}(x, x^\sigma) \equiv 0 \pmod{p}$  and  $\frac{\partial \Phi_p}{\partial Y}(x, x^\sigma) \not\equiv 0 \pmod{p}$ . Then to have the error  $e$  we must solve over  $\mathbb{Z}_q$  the following equation:

$$e^\sigma + Ae + B = 0.$$

with  $A \equiv 0 \pmod{p}$  and  $B \not\equiv 0 \pmod{p}$  called "**Artin-Schreier equation**" in [Gau04]. Set  $e = x + p^k \alpha$  with  $\alpha \in \mathbb{Z}_q$ , the error  $\alpha$  can be determine using Algorithm 2.1 (a general case of Harley's algorithm).

*Input*  $a, b \in \mathbb{Z}_q$  and the precision  $m$ .

*Output*  $e$  such that  $e^\sigma + ae + b \equiv 0 \pmod{p^N}$  with  $a = 0 \pmod{p}$

→ If  $N = 1$  Return  $e$  the unique root of  $e^p + b \equiv 0 \pmod{p}$ .

→  $x \leftarrow \text{ArtinSchreier}(a, b, N/2)$ .

→ Lift arbitrarily  $x$  at precision  $p^N$ .

→  $b' \leftarrow (x^\sigma + ax + b)/p^{N/2}$ .

→  $e \leftarrow \text{ArtinSchreier}(a, b', N/2)$ .

→ Return  $x + p^{N/2}e$ .

### Algorithm 2.1 Artin-Schreier

**2.4. Lift of the Weierstrass Equation.** In odd characteristic the short Weierstrass equations have two parameters that we denote  $A$  and  $B$ . Using the relation between the  $j$ -invariant and those parameters, given the  $j$ -invariant  $j(\tilde{E})$ , one can lift the equation of the elliptic curves defined over  $\mathbb{F}_q$  to  $\mathbb{Z}_q$ . Take an arbitrary lift of one parameter, then the equation between the lifted  $j$ -invariant and the second parameter provide a simple Newton algorithm to lift it. Furthermore in characteristic  $\geq 5$  Skjernaas [Skj03] has suggested to simply take  $A = 3\lambda$  and  $B = 2\lambda$  with

$$\lambda = \frac{j(E)}{1728 - j(E)}$$

This method is faster than the first. It needs only one inversion in  $\mathbb{Z}_q$  from the lifted  $j$ -invariant.

**2.5. The division polynomial.** If  $E/k$  is an elliptic curve with a short Weierstrass equation, and  $P = (x, y)$ , then  $\ell.P = \left(\frac{\xi_\ell(x)}{\psi_\ell^2(x)}, \frac{\omega_\ell(x, y)}{\psi_\ell^3(x, y)}\right)$  where  $\xi_\ell$  and  $\omega_\ell$  are expressible in terms of the  $\psi_{\ell-2}, \psi_{\ell-1}, \psi_\ell, \psi_{\ell+1}, \psi_{\ell+2}$ , and the  $\psi_\ell$  satisfy a recurrence relation expression  $\psi_{2\ell}$  and  $\psi_{2\ell+1}$  in term of he  $\psi_{\ell-2}, \psi_{\ell-1}, \psi_\ell, \psi_{\ell+1}, \psi_{\ell+2}$ . In practice, the recurrence formula simply come from computing  $\ell.P$  formally via the double and add algorithm. In particular, when  $\ell$  is odd, the roots of  $\psi_\ell(x)$  are exactly the elements  $x(P)$  for  $P \in E[\ell]$ .

In this article we will use a slightly different version of the division polynomial: we let  $\Psi_\ell(x) = \psi_\ell(x)$  when  $\ell$  is odd, and  $\Psi_\ell(x) = \psi_\ell(x)/2y$  when  $\ell$  is even. This reformulation is such that  $\Psi_\ell$  is always in  $k[x]$  whether  $\ell$  is even or odd. It is easy to adapt the recurrence formula to compute the  $\Psi_\ell$  directly.

In the following, we will need to compute  $\Psi_p(x)$  and  $\Psi'_p(x)$  for an elliptic curve  $\tilde{E}/\mathbb{Z}_q$  (at precision  $m$ ) modulo a polynomial  $H$  of degree  $d$ . In practice  $d$  will be equal to 1 when we want to evaluate  $\Psi_p$  on a point  $x_P$  (so  $H = (x - x_P)$ ), or  $d$  will be equal to  $(p-1)/2$  when we want to evaluate  $\Psi_p$  modulo  $\tilde{H}_p$  a candidate lift of  $H_p$ .

We remark that we can evaluate  $\Psi_p$  modulo  $H$  simply by evaluating the recurrence relation modulo  $H$ . Also from the recurrence relation on  $\Psi_\ell$ , we get a recurrence relation on  $\Psi'_\ell$ , so we can also evaluate it modulo  $H$ . We obtain

**Lemma 2.5.** *Given an elliptic curve  $\tilde{E}/\mathbb{Z}_q$  and a monic polynomial  $H(x)$  of degree  $d$ , we can evaluate  $\Psi_{\tilde{E},p}$  and  $\Psi'_{\tilde{E},p}$  modulo  $H$  at precision  $m$  in time  $\tilde{O}(dm \log q \log p) = \tilde{O}(dmn)$ .*

**2.6. Lifting the Verschiebung.** Since the Frobenius  $\pi_q$  is inseparable, we lift the Verschiebung  $\hat{\pi}_p$  over  $\mathbb{Z}_q$  by lifting its kernel.

We set  $E_{n-i} = E^{\sigma^i}$  and  $\pi_i$  is the isogeny between  $E_{i+1}$  and  $E_i$  defined by  $(x, y) \mapsto (x^\sigma, y^\sigma)$ . Then the Verschiebung  $\hat{\pi}_q$  decomposes as follow:

$$\hat{\pi}_q = \hat{\pi}_{n-1} \hat{\pi}_{n-2} \cdots \hat{\pi}_0.$$



$\ker(\hat{\pi})$  is a subgroup of order  $p$  of  $E[p]$  defined by the monic separable factor  $H_p$  of the  $p$ -division polynomial  $\Psi_p$  given by :

$$H_p(x) = \prod_{P \in \ker \hat{\sigma} \setminus \{O\}} (x - x(P))$$

Let  $\tilde{H}_p$  be the lift of  $H_p$  over  $\mathbb{Z}_q$ , then  $\tilde{H}_p$  is a monic factor of degree  $(p-1)/2$  of  $\Psi_p$  on  $\tilde{E}$  and  $\tilde{H}_p(x) = H_p(x) \pmod{p}$  is square free. Furthermore  $\Psi_p(x) \equiv H_p(x)^p \pmod{p}$  i.e modulo  $p$ , the factors  $H_p(x)$  and  $\Psi_p(x)/H_p(x)$  are not coprime modulo  $p$ .

T.Satoh introduced in [Sat00a, § 2] a variant of Hensel's lift that compute  $\tilde{H}_p$  over  $\mathbb{Z}_q$ . Let  $p$  be an odd prime, and suppose that we have a polynomial  $G$  in  $\mathbb{Z}_q[X]$  and  $h \in \mathbb{F}_q[X]$  a monic factor of the reduction of  $G$  modulo  $p$ . We assume that  $h(x)$  is separable and relatively prime with  $p^{-t}G'(x)$  where  $t = \text{ord}_p(G'(x))$ . Let  $u \in \mathbb{N}$  be such that  $G(x) \equiv q(x)h(x) \pmod{p^{u+t}}$ . Then the polynomial :

$$H(x) = h(x) + \left( \frac{G(x)}{G'(x)} h'(x) \pmod{h(x)} \right)$$

is a lift of  $h(x)$  at precision  $p^{2u}$  and  $G(x) \equiv Q(x)H(x) \pmod{p^v}$  where  $v = 2u + \min(t, u)$  (see [Sat00b]). This property provides an algorithm constructing a lift  $\tilde{h}$  with  $O((\deg h + \deg G)^2)$  arithmetic operations over  $\mathbb{Z}_q$  at precision  $p^{2n}$ .

Satoh then applies this construction to lift  $H_p$ , by [Sat00a, Lemma 3.7], in this case  $t = 1$ .

An alternative method when we are provided an étale point  $P$  of  $p$ -torsion is to lift the equation  $(p'+1).P = p'.P$  where  $p = 2p' + 1$  as in [MR20, Proposition A.7.], or to work with only the  $x$ -coordinate to simply use the standard Newton method to lift  $\Psi_p(x_p) = 0$ . This is faster than the euclidean extended GCD used in Satoh's formula above, we will revisit this in Section 4.

**2.7. Application to point counting.** When we have  $\tilde{E}$  at sufficient precision  $m$  (given by Hasse-Weil bounds), one can evaluate the action of the Verschiebung on the differential form  $\frac{dx}{y}$  as detailed by Satoh's diagram.

$$\begin{array}{ccc} \tilde{E} & \xrightarrow{\hat{\Sigma}} & \tilde{E}^{\hat{\Sigma}} \\ & \searrow \nu & \nearrow u \\ & \tilde{E}^\nu = \tilde{E}/\tilde{K} & \end{array}$$

Here the isogeny  $\nu$  is computed by Vélu's algorithm from the lift  $\tilde{H}_p$  of the kernel of the Verschiebung.

Since the isogeny  $\nu$  is normalized, the action of the isogeny  $\tilde{\pi}$  on the differential form of  $\tilde{E}$  is given by the isomorphism  $\pm u$  on  $\tilde{E}^\nu$ ; let us denote it by  $\lambda_1$ . Concretely, we have  $\tilde{\pi} = \pm u \circ \nu$ , and if  $u(x, y) = (u^2x, u^3y)$ ,  $\lambda_1 = \pm u$ .

On the other hand, when we consider the  $q^{th}$ -power Frobenius morphism decomposition:

$$\tilde{E} \longrightarrow \tilde{E}^{\Sigma} \longrightarrow \dots \longrightarrow \tilde{E}^{\Sigma^{n-1}}$$

The action on the differential forms along the cycle will be given by the successive conjugates of  $\lambda_1$ . Finally, by composition, the action of the dual endomorphism  $\tilde{\pi}_q$  of  $\tilde{\pi}_q$  on the main differential form of  $\tilde{E}$  is given by the product of all these conjugates, i.e. by the norm of  $\lambda_1$ . On the other hand the norm of  $N_{\mathbb{Q}_q/\mathbb{Q}_p}(\lambda_1)$  is simply given as the resultant of  $\lambda_1$  modulo  $M(X)$  in  $\mathbb{Q}_p[X]$ . This method due to Harley can be asymptotically done in quasi-linear time in the precision  $m$  using a fast GCD algorithm [CFA+06]. A slower alternative is to use the formula



*Input* Coefficients  $(A4, A6)$  of  $E$  an elliptic curve of  $\mathbb{F}_q$  with  $q = p^n$ ,  $n \in \mathbb{N}$ .

*Output* The Trace of Frobenius endomorphism of  $E$ .

- Using Algorithm 5.1, compute  $\tilde{E}$  at precision  $m = (n + 5)/2$  ;
- Compute the action  $\lambda_1$  of an isomorphism  $u : \tilde{E}^\nu \rightarrow \tilde{E}^{\hat{\Sigma}}$  ;
- Compute  $\lambda^2 = N_{\mathbb{Q}_q/\mathbb{Q}_p}(\lambda_1^2)$  ;
- Compute  $\lambda$  the correct square root from  $\lambda^2$  and  $t = \lambda + q/\lambda \pmod q$  such that  $|t| < 2\sqrt{q}$  ;
- Return  $\chi(X) = X^2 - t \cdot X + q$  .

---

**Algorithm 2.2** Computing the characteristic polynomial of ordinary elliptic curve  $E$

---

$N_{\mathbb{Q}_q/\mathbb{Q}_p}(c) = \exp(\text{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(\log c))$  using a specific implementation to compute it in time  $O(m^{3/2}n)$  (available in [PAR19]).

Since we only have  $\lambda_1$  up to a sign, taking its norm  $\lambda$  and then computing the trace  $t = \lambda + q/\lambda$  only give  $t$  up to a sign. One can use Hasse's invariant to get the correct sign, see Section 4.2. Let  $\chi(X) = X^2 - t \cdot X + q$  be characteristic polynomial of the Frobenius of  $E$ , Hasse-Weil bound states  $|t| < 2\sqrt{q}$ . On the other hand we have  $\#E(\mathbb{F}_q) = \chi(1)$ . Then we deduce the following result:

**Theorem 2.6.** *Let  $E/\mathbb{F}_q$  be an ordinary elliptic curve. Given the canonical lift  $\tilde{E}/\mathbb{Z}_q$  and the lift  $\tilde{H}_p$  of the kernel of the Verschiebung to precision  $m$ , one can compute the trace of the Frobenius to  $p$ -adic precision  $m$  in time  $\tilde{O}(mnp)$ .*

*In particular, for point counting where we need  $m = O(n)$ , the complexity to compute  $\chi_\pi$  once we have  $\tilde{E}$  and  $\tilde{H}_p$  to precision  $m$  is  $\tilde{O}(pn^2)$ .*

In the rest of this paper, we will explain how we can compute  $\tilde{E}$  and  $\tilde{H}_p$  to precision  $m$  in time  $\tilde{O}(mnp)$  rather than in time  $\tilde{O}(mnp^2)$ . By Theorem 2.6, this will show that we have a point counting algorithm in time  $\tilde{O}(n^2p)$ .

We also remark that we can bypass the computation of  $\tilde{E}^{\hat{\Sigma}}$  (since  $\hat{\Sigma}$  is typically more expensive to compute than  $\Sigma$ ) by applying the above method to  $\tilde{E}^{\hat{\Sigma}}$ , the canonical lift of  $E^\sigma$  instead.

### 3. REVISITING NEWTON'S METHOD

Let  $F(X)$  be a multivariate polynomial system defined over  $\mathbb{Z}_q$ , and suppose that we have a solution  $x$  modulo  $p$  (in other words, at precision 1) of the equation  $F(x) = 0$  (modulo  $p$ ). Assume furthermore that  $dF(x)$  is invertible modulo  $p$ . Then there is a unique lift  $\tilde{x}$  of  $x$  in  $\mathbb{Z}_q$  such that  $F(\tilde{x}) = 0$  and  $\tilde{x} = x$  modulo  $p$ . Newton's method show that  $\tilde{x}$  can be approximated by the sequence

$$(1) \quad x_0 = x, \quad x_{2k} = x_k - dF(x_k)^{-1}F(x_k).$$

A standard computation shows that  $x_k$  approximates  $\tilde{x}$  to precision  $m = 2^k$  and that  $F(x_k) = 0$  modulo  $p^m$ .

Our trivial, but key remark which is at the core of this article, is that to use Newton's method we do not need to know  $F$ , we only need to be able to evaluate  $F$  at some precision  $m$ . Indeed from Equation (1) it is clear that we only need to be able to evaluate  $F$  and  $dF$ . But we can recover  $dF$  from evaluations of  $F$  at suitable points.

We illustrate this when  $F(X)$  is univariate. Then modulo  $p^{2m}$ ,  $F(x + p^m y) = F(x) + F'(x)p^m y$ , hence  $F'(x) = (F(x + p^m) - F(x))/p^m$  modulo  $p^m$ . We can thus recover  $F'(x)$  modulo  $p^m$  from two evaluations of  $F$  at precision  $2m$ . The Newton process can thus be done as follow: given

the solution  $x_m$  at precision  $m$ , we evaluate  $F(x_m)$  and  $F(x_m + p^m)$  at precision  $2m$ . Then 
$$x_{2m} = x_m - \frac{F(x_m)}{(F(x_m + p^m) - F(x_m))/p^m}.$$

More generally, when  $F$  has  $N$ -variable, we can recover the Jacobian  $dF(x)$  at precision  $m$  in  $N + 1$  evaluations of  $F$  at precision  $2m$ .

We have proved:

**Lemma 3.1.** *Given a multivariate polynomial system  $F(X)$  in  $N$  variables and  $N$  equations, and a solution  $x_0$  modulo  $p$  of the equation  $F(x) = 0$  modulo  $p$  such that  $dF(x_0)$  is invertible modulo  $p$ . Let  $C(m, \mathbb{Z}_q)$  be the cost of evaluating  $F$  at a point  $x$  at precision  $m$  and  $M(m, \mathbb{Z}_q)$  be the cost of doing the standard arithmetic operations in  $\mathbb{Z}_q$  at precision  $m$ , and assume that both  $C(m)$  and  $M(m)$  are superlinear.*

*Then one can compute the unique lift  $\tilde{x}$  of  $x_0$  such that  $F(\tilde{x}) = 0$  to precision  $m$  in time  $O(N \cdot C(2m, \mathbb{Z}_q) + N \cdot M(2m, \mathbb{Z}_q))$ .*

**Remark 3.2.** We note that if we have an approximation  $x_0$  of  $\tilde{x}$  to precision  $m$ , then for our method (and the convergence), we only need that  $F$  is analytic at  $x_0$  on the ball of center  $x_0$  and radius  $\|p^m\|$ .

More generally, Newton's algorithm will converge whenever we have a  $x_0$  modulo  $p^{e+1}$  such that  $f(x_0) = 0$  modulo  $p^{2e+1}$  and  $p^e dF(x_0)$  is invertible. Iterating the Newton process then gives  $\tilde{x}$  modulo  $p^{e+2^k}$  such that  $f(\tilde{x}) = 0$  modulo  $p^{2e+2^k}$ .

When this is not the case, we need to push the Taylor expansion of  $F$  further:

$$F(x + ep^k) = p^k dF(x) \cdot {}^t e_i + p^{2k} e_i \cdot d^2 F(x, x) \cdot {}^t e_i + O(p^{3k}).$$

Let  $J(x) = dF(x)$  be the Jacobian, and  $H(x) = d^2 F(x, x)$  be the Hessian matrix, we explain how to evaluate them to precision  $m$ . We assume here for simplicity that  $N = 2$  and  $p > 2$ . Set  $e_1 = (1, 0)$ ,  $e_2 = (0, 1)$  and  $e_5 = (1, 1)$ , set  $x_1 = x + e_1 p^m$ ,  $x_2 = x + e_2 p^m$ ,  $x_3 = x - e_1 p^m$ ,  $x_4 = x - e_2 p^m$  and  $x_5 = x + e_5 p^m$ , and evaluate  $F(x_i)$  modulo  $p^{3m}$ .

We have modulo  $p^{2m}$ :

$$J_X(x) = \frac{F(x_1) - F(x_3)}{2p^m} \quad \text{and} \quad J_Y(x) = \frac{F(x_2) - F(x_4)}{2p^m}$$

and modulo  $p^m$ :

$$H_X(x) = \frac{F(x_1) - J_X(x)p^m}{p^{2m}}, \quad H_Y(x) = \frac{F(x_2) - J_Y(x)p^m}{p^{2m}}$$

$$H_{XY}(x) = \frac{F(x_5) - F(x) - J_X(x)p^m - J_Y(x)p^m - H_X(x)p^{2m} - H_Y(x)p^{2m}}{p^{2m}}.$$

More generally, in  $N$  variables we may compute  $d^k F(x)$  at precision  $m$  by  $O(k + N^{k+1})$  evaluations of  $F$  at precision  $km$  when  $p$  is large enough.

#### 4. LIFTING THE ÉTALE POINTS OF $p$ -TORSION

Let  $\tilde{E}/\mathbb{Z}_q$  be a (non necessarily canonic here) lift of an ordinary elliptic curve  $E/\mathbb{F}_q$ . In this section we will denote the canonical lift by  $E^\uparrow$ .

In this section, we explain how to compute the polynomial  $H_p$  which parametrizes  $E[p]_{\text{ét}}$  (this is also the kernel of the Verschiebung) and how to lift it to  $\tilde{E}$  using Section 3. We also explain how to find an étale point  $P \in E[p]$  and how to lift it.

We first note that when  $\tilde{E}$  is an arbitrary lift of  $E$ , there is an obstruction to lifting an étale point of  $p$ -torsion  $P$ : in general  $\tilde{E}[p]$  may not have points living in an unramified extension of  $\mathbb{Z}_q$ , in particular even if  $P$  is rational, a lift of  $P$  to  $\tilde{E}[p](\mathbb{Z}_q)$  will not exist. This obstruction vanish if and only if  $j(\tilde{E}) = j(E^\uparrow) \pmod{p^2}$ :

**Proposition 4.1.** *Let  $\tilde{E}/\mathbb{Z}_q$  be an arbitrary lift of  $E/\mathbb{F}_q$ , and let  $E^\dagger/\mathbb{Z}_q$  be the canonical lift of  $E$ . Let  $\mathbb{Z}_q^{\text{ur}}$  be the maximal unramified extension of  $\mathbb{Z}_q$ . The following are equivalent:*

- (1)  $\tilde{E}[p](\mathbb{Z}_q^{\text{ur}}) \neq \{0_E\}$ ;
- (2)  $\tilde{E}[p](\mathbb{Z}_q^{\text{ur}})$  is a lift of  $E[p]_{\text{et}}$ ;
- (3)  $\mathbb{Z}_q(\tilde{E}[p])$  is tamely ramified;
- (4)  $j(\tilde{E}) = j(E^\dagger) \pmod{p^2}$ .

If these conditions are satisfied, and  $\mathbb{F}_{q^e}$  is the smallest extension of  $\mathbb{F}_q$  where the points of  $E[p]_{\text{et}}$  are defined, then  $\tilde{E}[p] = \tilde{E}^0[p] \oplus \tilde{E}[p](\mathbb{Z}_{q^e})$  where  $\tilde{E}^0$  is the relative connected component of  $E$  (ie the kernel of the reduction map  $\tilde{E} \rightarrow E$ ), and the points of  $\tilde{E}^0[p]$  live in the tamely ramified extension of  $\mathbb{Z}_{q^e}$  given by adjoining a  $p$ -root of unity  $\zeta_p$ . Furthermore, if  $P \in \tilde{E}[p](\mathbb{Z}_q^{\text{ur}})$ , then  $\Psi'_p(P)$  is of valuation 1.

*Proof.* We have a connected étale exact sequence [Tat97]:

$$0 \rightarrow \tilde{E}^0 \rightarrow \tilde{E} \rightarrow \tilde{E}^{\text{et}} \rightarrow 0.$$

This exact sequence commutes with specialisation, so since  $\text{Spec } \mathbb{Z}_q$  is connected,  $\tilde{E}^0$  is exactly the kernel of the projection map  $\tilde{E} \rightarrow E$ . In particular, since  $\tilde{E}^{\text{et}}[p]$  is étale and  $\mathbb{Z}_q$  is complete hence Henselian, it is the unique étale lift of  $E[p]_{\text{et}}$ , and  $\tilde{E}^0[p]$  is a lift of  $E[p]_{\text{loc}}$  which is of multiplicative type (since it is the Cartier dual of  $E[p]_{\text{et}}$ ), hence its points live in a ramified extension of  $\mathbb{Z}_q$ . So if  $\tilde{P} \in \tilde{E}[p](\mathbb{Z}_q^{\text{ur}}) \neq 0_{\tilde{E}}$ , the subgroup generated by  $\tilde{P}$  induces a splitting  $\tilde{E}[p] = \tilde{E}^0[p] \oplus \tilde{E}^{\text{et}}[p]$ , in particular  $\tilde{P} \notin \tilde{E}^0[p]$ . This proves the equivalence of (1) and (2). The rest of the equivalences are from [Sat00b, Theorem 3.1]. Furthermore we have  $\tilde{E}[p](\mathbb{Z}_q^{\text{ur}}) = \tilde{E}^{\text{et}}[p](\mathbb{Z}_q^{\text{ur}}) = \tilde{E}^{\text{et}}[p](\mathbb{Z}_{q^e})$ , and since  $\tilde{E}^0[p]$  is the Cartier dual of  $\tilde{E}^{\text{et}}$  its points live in  $\mathbb{Q}_q(\zeta_p)$ .

Finally,  $\Psi'_p(P) = 1$  by Satoh's lemma [Sat00a, Lemma 3.7].  $\square$

**4.1. Computing the kernel of the Verschiebung.** To apply Section 2.6, we first need to compute the kernel  $H_p$  of the Verschiebung (or a rational point in this kernel).

We have  $\Psi_p = H_p^p$ , so an easy method is to compute  $\Psi_p$  using the recursive formula for division polynomials to get  $H_p$ . But  $\Psi_p$  is of degree  $p^2$ , so this will cost  $\tilde{O}(p^2 n)$  operations.

Let  $\hat{\pi}$  be the Verschiebung. By definition  $[p] = \pi\hat{\pi} = \hat{\pi}\pi$ , so we have  $\hat{\pi}(\pi(P)) = [p].P$ . In particular we can efficiently evaluate the Verschiebung on the point  $\pi(P)$ . We can thus recover the Verschiebung by interpolation, from which we get the kernel.

More precisely we only need to work with  $x$ -coordinates. We can then sample  $p$ -random points  $x_p \in E^{\hat{\sigma}}(\mathbb{F}_q)/\pm 1$ , and compute the values  $p.x_p$  in  $x$ -coordinates only. Let  $R(x)$  be the rational fraction of degree  $O(p)$  interpolating the points  $(\pi(x_p), p.x_p)$ . Then the kernel  $H_p$  of the Verschiebung is simply the denominator of  $R$ .

In summary:

**Lemma 4.2.** *Let  $E/\mathbb{F}_q$  be an ordinary elliptic curve. The kernel  $H_p(x)$  of the (small) Verschiebung can be computed in time  $\tilde{O}(p \log q) = \tilde{O}(pn)$ .*

**4.2. Finding an étale point of torsion.** If we furthermore need the  $x$ -coordinate of an étale point  $P$  of  $p$ -torsion, we need to find a root of  $H_p$ . First we need to compute the degree  $e$  of the extension where the étale points of  $p$ -torsion live. Assume that we know  $\lambda$ , the invertible eigenvalue of the Frobenius modulo  $p$ . Then  $\sigma(P) = \lambda.P$ , so  $e$  is the order of  $\lambda$ .

There are two methods to find  $\lambda$  to precision 1. The first one is to use Hasse's formula. Using the recurrence formula to compute the Hasse invariant  $A_q$  (see [Sil86, p. V.4.1]), this costs  $\tilde{O}(n^2 + np)$  operations:  $\tilde{O}(np)$  to compute  $A_p$ , then  $\tilde{O}(\log^2 q) = \tilde{O}(n^2)$  to compute  $A_q$ .

The other approach evaluates the Verschiebung from its kernel  $H_p$  using Vélú's formula, and look at the action on the differentials (ie we apply Satoh's algorithm at precision  $m = 1$ , so without lifting), as in Section 2.7. This costs  $\tilde{O}(np)$  operations, but this only recovers  $\pm\lambda$ .

Indeed, we compute an isomorphism  $u : E/H_p \simeq E^{\hat{\sigma}}, (x, y) \mapsto (u^2x, u^3y)$ , so if  $\phi : E \rightarrow E/H_p$  is given by Vélú's formula, the Verschiebung is equal to  $\pm u \circ \phi$ . To know the correct sign, we need to stop working in  $x$ -coordinate only and take a random point  $P \in E(\mathbb{F}_q)$  and check whether  $[p]\hat{\sigma}(P) = u \circ \phi(P)$  or  $[p]\hat{\sigma}(P) = -u \circ \phi(P)$ . Then replacing  $u$  by  $-u$  if necessary, we have that  $\lambda = N_{\mathbb{F}_q/\mathbb{F}_p}(u)$  since  $\phi$  is normalised. To take  $P$  we need to compute a square root, so this costs  $\tilde{O}(\log^2 q) = \tilde{O}(n^2)$ , and the total cost to recover  $e$  exactly (rather than potentially  $2e$ ) is  $\tilde{O}(n^2 + np)$  operations, like the computation of the Hasse invariant.

The factorisation of  $H_p$  using an equal degree factorisation algorithm then costs  $\tilde{O}(p \log^2 q) = \tilde{O}(pn^2)$ . We note that without the knowledge of  $e$ , we would need to use a distinct degree factorisation algorithm instead, which would cost  $\tilde{O}(p^{1.5}n + pn^2)$  by [KU11]. In summary:

**Lemma 4.3.** *Let  $E/\mathbb{F}_q$  be an ordinary elliptic curve. The kernel  $H_p(x)$  of the (small) Verschiebung can be computed and factorized in time  $\tilde{O}(pn^2)$ .*

There is a faster method when we already know  $N = \#E(\mathbb{F}_q)$ . Compute  $e$  as above, and  $N_e = \#E(\mathbb{F}_{q^e})$ . Take a random point  $Q \in E(\mathbb{F}_{q^e})$  and multiply by the cofactor:  $P = N_e/p \cdot Q$ . If  $P \neq 0_0$  we have found a point of  $p$ -torsion. A random point  $Q$  can be taken by taking a random  $x_Q$  and trying to find a square root of  $x_Q^3 + ax_Q + b$ . We can also work in  $x$ -coordinates only, this gains a square root. In any case, the total cost of this method is  $\tilde{O}(\log^2 q^e) = \tilde{O}(e^2 n^2)$ .

**4.3. Lifting a point of  $p$ -torsion.** We now assume that we are given a lift  $\tilde{E}$  that satisfy the equivalent conditions of Proposition 4.1.

Given a point  $P$  of  $p$ -torsion on  $E$ , to lift it to  $\tilde{E}$  we apply Lemma 3.1 to the equation  $p\tilde{P} = 0_E$ . To stay in affine coordinates, we can rewrite this equation as  $(p' + 1)\tilde{P} = -p'\tilde{P}$  for  $p = 2p' + 1$ .

Evaluating this equation by a double and add algorithm takes  $O(\log p)$  operations in  $\mathbb{Z}_q$  (at a given precision  $m$ ), hence by Lemma 3.1 we can compute  $\tilde{P}$  to precision  $m$  in time  $\tilde{O}(nm)$ .

Remark that the  $p$ -torsion  $P$  points is defined equivalently by systems of the form:

$$\begin{cases} f(x, y) = 0 \\ \Psi_p(x) = 0 \end{cases} \quad \text{or} \quad \begin{cases} f(x, y) = 0 \\ g(x, y) = 0 \end{cases}$$

where  $g(x, y)$  is one of the equation  $[p' + 1]P = -[p']P$  such that  $p = 2p' + 1$ .

Since  $p \neq 2$ , we have  $\frac{\partial f}{\partial y}(P)$  non nul modulo  $p$ . The Jacobian of the system is given by:

$$\begin{pmatrix} \frac{\partial f}{\partial x}(x, y) & \frac{\partial f}{\partial y}(x, y) \\ \Psi'_p(x) & 0 \end{pmatrix}$$

Then using Satoh's lemma [Sat00a, Lemma 3.7], we conclude that the valuation the determinant of the Jacobian of those system at  $P$  is 1:

$$\text{it has the form } \begin{pmatrix} \star & \star \\ p & 0 \end{pmatrix} \text{ at } P$$

Thus in the Newton's lifting steps, we lost 1 precision on the coordinates of  $\tilde{P}$ . Also to bootstrap at precision 1, it seems like we would need to compute the Hessian.

Fortunately, the situation simplifies if we only try to lift the  $x$ -coordinate of  $P$ , the system then becomes  $\Psi_p(x) = 0$ . We never compute  $\Psi_p$  but evaluate it on  $x$  directly via the double and add formula for  $x$ -coordinates (in other words via the standard recurrence formula for the division polynomials) by Lemma 2.5. However, our lift is such that  $\Psi'_p(x_{\tilde{P}})$  is of valuation 1 and

$\Psi_p(x_{\tilde{P}})$  is only of valuation 2 (by Proposition 4.1), not 3 as needed to bootstrap the Newton method, see Remark 3.2. But since  $\Psi''_p(x_{\tilde{P}}) = 0$  modulo  $p$  (because  $\Psi_p = H_p^p$ , the first iteration of the Newton method does still allow to go to precision 3, as remarked in [Rob21a, Aside 6.2.2]). We can then apply Remark 3.2: we compute  $x_{\tilde{P}}$  modulo  $p^k$  such that  $\Psi_p(x_{\tilde{P}}) = 0$  modulo  $p^{k+1}$ . We can then lift  $y_P$  by solving the square root via Newton's algorithm.

In summary:

**Lemma 4.4.** *Let  $\tilde{E}/\mathbb{Z}_q$  be a lift of  $E$  that satisfy the conditions of Proposition 4.1, and let  $P$  be an étale point of  $p$ -torsion on  $E$  which lives in  $\mathbb{F}_{q^e}$ . Then  $P$  can be lifted to a point of  $p$ -torsion  $\tilde{P} \in \tilde{E}[p](\mathbb{Z}_{q^e})$  to precision  $m$  in time  $\tilde{O}(m \log q \log p) = \tilde{O}(mn)$ .*

**4.4. Lifting all the étale  $p$ -Torsion.** An alternative is to lift directly the kernel of the Verschiebung  $H_p$ . Suppose that we are given  $\tilde{H}_p$  at precision  $k$ , and we want to compute it at precision  $2k$ .

First we note that by employing the same strategy as in Section 4.3 but working over the algebra  $A_p = \mathbb{F}_q[u]/H_p(u)$  rather than over  $\mathbb{F}_{q^e}$ , we can find a lift  $\tilde{P} = u + p.a_1(u) + p^2.a_2(u) + \dots$  of the formal point of  $p$ -torsion  $P : x = u$ . Notably,  $\tilde{P}$  encodes simultaneously the lifts of all points of  $p$ -torsion: if  $P_\lambda$  is the point of  $p$ -torsion with  $x$ -coordinate given by the root  $\lambda$  of  $H_p$ , its lift  $\tilde{P}_\lambda$  is given by  $\lambda + p.u_1(\lambda) + p^2.u_2(\lambda) + \dots$ .

Then  $\tilde{H}_p(x)$  is given by the resultant  $\text{Res}_u(x - u, \tilde{P})$ . But it is not clear if this resultant can be computed in quasi-linear time (the best generic algorithm in [Vil18] is not quasi-linear, but in our situation the roots of  $\tilde{H}_p$  are deformations of the roots of  $H_p$  so there may be more efficient algorithms.)

So rather than lifting the formal point  $P : x = u$  over  $A_p$ , we simply lift  $\tilde{H}_p$  directly. We give two methods.

The first is to use Section 3 applied to the equation  $\Psi_p \bmod \tilde{H}_p = 0 \bmod p^{2k}$  (where  $2k$  is our target precision).

Indeed by Lemma 2.5,  $\Psi_p$  can be evaluated modulo our candidate polynomial  $\tilde{H}_p^*$  via the recurrence formula in quasi-linear time (so we never need to compute it fully, only modulo a polynomial of degree  $p$ ).

The Newton formula is as follow: take an arbitrary lift  $\tilde{H}_p^*$ , let  $a = \Psi_p \bmod \tilde{H}_p^*$  and  $b = \Psi_p \bmod (\tilde{H}_p^* + p)$ . Then the derivative of our Newton process is given by  $c = (b - a)/p^k$ , and we solve the equation  $a + cp^k Q = 0 \bmod (\tilde{H}_p^*, p^{2k})$  (since the equation is valid at precision  $k$ , this equation does not depend on the choice of  $\tilde{H}_p^*$ ). The correct lift is then  $\tilde{H}_p = \tilde{H}_p^* + p^k Q$ .

The second one is to use the strategy of Section 2.6. Given  $\tilde{H}_p$  at precision  $k$ , take an arbitrary lift  $\tilde{H}_p^*$  to precision  $2k + 1$ , then we have

$$\tilde{H}_p = \tilde{H}_p^* + e \quad \text{with} \quad e = \frac{\Psi_p \cdot \tilde{H}_p^{*'} - p}{\Psi_p'} \bmod \tilde{H}_p^*.$$

We can use Lemma 2.5 to compute  $e$  in quasi-linear time.

In summary both methods give:

**Proposition 4.5.** *Given an ordinary elliptic curve  $E/\mathbb{F}_q$ , and a lift (not necessarily canonical)  $\tilde{E}$  at precision  $m$  that satisfy the conditions of Proposition 4.1, the kernel  $H_p$  of the Verschiebung can be lifted to precision  $m$  in quasi-linear time  $\tilde{O}(mp \log q) = \tilde{O}(pmn)$ .*

**Remark 4.6.** As for Section 4.3, when  $\tilde{E}$  is given at precision  $m$ ,  $\tilde{H}_p$  is only determined to precision  $m - 1$ .

It is easy to see that we can extend the methods of this section to lift to  $\tilde{E}$  a subgroup  $G$  of degree  $d$  of  $E[\ell]$ , when  $p \nmid \ell$ . (In this case there is no restriction on  $\tilde{E}$  since  $E[\ell]$  is étale.)

This subgroup is defined by a polynomial  $H_G(x)$  (say when  $\ell$  is odd) of degree  $(d-1)/2$ . The standard method would be to lift  $H_G(X)$  as a factor of  $\chi_{\ell, \tilde{E}}(X)$ , which would cost  $\tilde{O}(\ell^2 m \log q)$  at precision  $m$ . Our method only computes  $\chi_\ell$  modulo (potential) lifts of  $H_G$ , hence only cost  $\tilde{O}(d \log \ell m \log q) = \tilde{O}(d \log \ell m n)$  (where the  $\log \ell$  comes from the recurrence formula for  $\Psi_\ell$  may not be absorbed in the  $\tilde{O}$  notation here).

## 5. COMPUTING THE CANONICAL LIFT WITHOUT THE USE MODULAR POLYNOMIALS

In this section we will focus on the case where  $p$  is odd for simplicity.

**Lemma 5.1.** *Let  $E$  an ordinary elliptic curve over  $\mathbb{F}_q$ , then  $\tilde{E}$  is the unique elliptic curve up to isomorphism over  $\mathbb{Z}_q$  such that.*

- $E$  is the reduction of  $\tilde{E}$  modulo  $p$ ,
- Let  $K \subset \tilde{E}(\mathbb{Q}_q^{\text{un}})$  be such that  $K$  reduces to  $E[p]_{\text{et}}$  modulo  $p$  and  $\nu : \tilde{E} \rightarrow \tilde{E}/K$ . Then  $j(\tilde{E}^\nu) = j(\tilde{E})^\Sigma$

*Proof.* Immediate by Section 2 and Theorem 2.2, □

We can then apply Lemma 3.1 to the equation of Lemma 5.1 to compute the  $j$ -invariant  $J$  of the canonical lift. We first note that Proposition 4.1 gives a convenient criteria to compute the canonical lift  $\tilde{E}$  to precision 2.

**Lemma 5.2.** *Let  $E/\mathbb{F}_q$  be an ordinary elliptic curve,  $P$  a point of  $p$ -torsion on  $E$ , and  $H_p$  the kernel of the Verschiebung. Let  $\tilde{E}/\mathbb{Z}_q$  be a lift of  $E$ . Then  $j(\tilde{E}) = j(E^\uparrow) \pmod{p^2}$  if and only if  $\Psi_{\tilde{E}, p}(P) = 0 \pmod{p^2}$ , if and only if  $\Psi_{\tilde{E}, p} = 0 \pmod{(p^2, H_p)}$ .*

*Proof.* We first note that the value of  $\Psi_{\tilde{E}, p}(P)$  does not depend on the choice of lift  $\tilde{P}$  of  $P$  to precision 2 since  $\Psi'_p(P) = 0 \pmod{p}$ . The same hold for  $\Psi_{\tilde{E}, p}$  modulo  $H_p$ .

By Section 4, is  $\Psi_{\tilde{E}, p}(P) = 0 \pmod{p^2}$  then Newton's method lifts  $P$  to a point of  $p$ -torsion on  $\tilde{E}$ , alternatively the existence of a point of  $p$ -torsion on  $\tilde{E}$  is given by [Sat00b, Theorem 3.1].

The lemma is then a direct application of Proposition 4.1. □

So  $\tilde{E} \pmod{p^2}$  correspond to the unique elliptic curve (up to isomorphism)  $\tilde{E} \pmod{p^2}$  such that  $\Psi_{\tilde{E}, p}(P) = 0$ . Such we look for  $\tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b} \pmod{p^2}$  such that  $\Psi_{\tilde{E}, p}(P) = 0$ . Taking  $\tilde{a}$  an arbitrary lift of  $a$ , we look for  $\tilde{b} = b_0 + pb_1$ , and we solve for  $b_1$  by using the methods of Section 3. If we have  $H_p$  instead, we do the same computation using the equation  $\Psi_{\tilde{E}, p} \%_{H_p} = 0 \pmod{p^2}$ .

Assume that we have  $J$  at  $p$ -adic precision  $k \geq 2$ , we want to find it at precision  $2k$ . We assume here that we are given  $H_p$ , we explain how to adjust the algorithm when we are given a point of  $p$ -torsion  $P$  instead afterwards.

We let  $F(X)$  be the following process (at precision  $2k$ ): given  $x$  such that  $x = j(E) \pmod{p}$ , we construct the elliptic curve  $\mathcal{E}$  with  $j$ -invariant  $x$ , we let  $\tilde{H}_p$  be the lift of  $H_p$  to  $\mathcal{E}$ , and  $\mathcal{E}^\nu$  the isogenous variety  $\mathcal{E}/\tilde{H}_p$ . Then  $x = j(\mathcal{E})$  is the lift we look for whenever  $F(x) = x^\Sigma$ .

We can evaluate  $F(X)$  using Vélú's formula and Section 4, hence we can also evaluate  $F'(X)$  by Section 3.

**Lemma 5.3.** *Let  $J$  satisfy  $F(J) = J^\Sigma$  at precision  $k \geq 2$ , and take an arbitrary lift at precision  $2k$ . Let  $A = F(J)$  and  $B = F'(J)$ . Then  $F(J + ep^k) = A + Bp^k e$ , where  $B$  is of valuation  $-1$ .*

*Proof.* By definition of  $F$ , if  $J' = J + p^k e$ , we have  $\Phi_p(J', F(J')) = 0 \pmod{p^{2k}}$ . Write  $F(J') = F(J) + p^k e'$ , then  $\Phi_p(J, F(J)) + \partial \Phi_p / \partial_x (J, F(J)) p^k e + \partial \Phi_p / \partial_y (J, F(J)) p^k e' = 0 \pmod{p^{2k}}$ ,

*Input*  $E$  an elliptic curve of  $\mathbb{F}_q$  with  $q = p^n$ ,  $n \in \mathbb{N}$ .

*Output* The canonical lift of  $E$  at precision  $m$ .

- Compute  $H_p$  over  $\mathbb{F}_q$  using Section 4.1 ;
- Compute  $\tilde{E}$  at precision 2 using the equation  $\tilde{\Psi}_p \bmod H_p = 0$  at precision 2 ;
- Compute  $\tilde{H}_p \bmod p^{2+1}$ .
- $k = 1$
- while  $k < \lceil (m-1)/2 \rceil$  ;
  - a. Compute at precision  $2(k+1)$  two lifts of the curve  $\tilde{E} \bmod p^{k+1}$  ;
  - b. Compute  $\tilde{H}_p \bmod p^{2k+1}$  on these two curves using Section 4.4.
  - c. Solve the equation  $j(\tilde{E}^\nu) = j(\tilde{E})^{\tilde{\Sigma}}$  to recover the curve  $\tilde{E} \bmod p^{2k+1}$  ;
  - d.  $k = 2k$ ;
- Return  $\tilde{E}$  at precision  $m$  .

---

**Algorithm 5.1** Computing the canonical lift by lifting the étale  $p$ -torsion

---

hence  $B = \partial\Phi_p/\partial_x(J, F(J))/\partial\Phi_p/\partial_y(J, F(J))$  is of valuation  $-1$  by by Kronecker's formula (see Section 2.3 and Lemma 2.4).  $\square$

We look for a lift of the form  $J + p^k e$ , and we want:

$$F(J + p^k e) = A + B.e.p^k = J^{\tilde{\Sigma}} + e^{\tilde{\Sigma}}.p^k = A^{\tilde{\Sigma}} + B^{\tilde{\Sigma}}p^k e^{\tilde{\Sigma}}.$$

Since  $B$  is of valuation  $-1$ , evaluating  $F(X)$  only make sense modulo  $p^{2k-1}$ . Concretely this stems from the fact that given  $\tilde{E}$  at precision  $2k$ , we can only compute  $\tilde{H}_p$  at precision  $2k-1$ , so the corresponding isogeny at precision  $2k-1$ . So we solve  $F(J + p^k e) = A + (Bp)p^{k-1}e = J^{\tilde{\Sigma}} + e^{\tilde{\Sigma}}p^k \bmod p^{2k-1}$ .

By applying the Frobenius  $\Sigma$ , we get:

$$A^\Sigma + B^\Sigma.e^\Sigma.p^k = J + e.p^k$$

So dividing by  $(pB)p^{k-1}$  (recall that  $pB$  is invertible), we obtain an equation of the form:

$$e^\Sigma + a.e + b = 0 \bmod p^k$$

. where  $a = 0$  modulo  $p$ . We then solve this equation using Algorithm 2.1.

This proves Theorem 1.1. The resulting algorithm is given in Section 5.

**Computing the canonical lift from lifting a point of  $p$ -torsion.** Instead of lifting  $H_p$  to compute the isogeny, we could also lift a point of  $p$ -torsion  $P$  directly and use an isogeny algorithm that takes a point of the kernel as input to compute the isogenous curve  $\mathcal{E}^\nu$ . This second strategy gives the complexity stated by Theorem 1.2, the algorithms are summarized in Algorithms 5.2 and 5.3.

To illustrate the flexibility of Section 3, rather than working with the  $j$ -invariant, we also illustrate a variant which works directly with the coefficients of  $\tilde{E}$ .

Suppose at precision  $k$  we have  $E : y^2 = x^3 + Ax + B$  and  $P(x_p, y_p) \in E[p] - \{\mathcal{O}\}$ .

Let  $(e, r)$  be the couple of error such that:  $x_{\tilde{P}} - x_P = e.p^k$  and  $y_{\tilde{P}} - y_P = r.p^k$ , then we can obtain a lift the coefficients  $A$  and  $B$  by taking  $A$  and  $B + \theta.p^k$ . These three errors  $e$ ,  $r$  and  $\theta$



*Input* Coefficients  $(A4, A6)$ ,  $p$ -torsion  $P$  and integer  $m$  the precision.

*Output* Coefficients  $(\tilde{A}2, \tilde{A}6)$  at precision  $m$ .

- $k = 1$ ;
- Use Initialization Phase (Lemma 5.2) to compute  $\tilde{J}$  at precision 2;
- While  $(2 \leq k \leq (m + 1)/2)$  ;
  - a. Use Algorithm 5.3 to compute  $\tilde{J}$  at precision  $2k - 1$ ;
  - b. Compute the lift  $(\tilde{A}4, \tilde{A}6)$  of coefficients at  $2k - 1$  using  $\tilde{J}$  and the method Section 2.4 ;
  - c.  $k = 2k - 1$ ;
- Return  $(\tilde{A}4, \tilde{A}6)$  .

---

**Algorithm 5.2** Lifting the coefficients  $(A4, A6)$  of an ordinary elliptic curve  $E$

---

constitute the unique root of system given by:

$$\begin{cases} \tilde{P} \in \tilde{E}, \\ \Psi_p(x_{\tilde{P}}) = 0, \\ j(\tilde{E}^\nu) = j(\tilde{E})^{\tilde{\Sigma}} \end{cases}$$

Then using the first equation we get:  $r = \frac{1}{2y_P} [(x_P^3 + A.x_P + B - y_P^2)/p^k + (3.e.x_P^2 + A.e + \theta)]$ .

And using the second equation, one can extract  $p.e$  from  $\Psi_p(x_p + e.p^k, A, B + \theta.p^k) = 0$  (since from Satoh's lemma we have  $\Psi'_p(x_p + e.p^k)$  has valuation 1).

On other hand, let  $A_v$  and  $B_v$  be the coefficients of the  $p$ -isogenous curve given by the Vélú's formula from the input  $(A, B + \theta.p^k, P_{e,r})$  at the precision  $2k$  where  $P_{e,r} = (x_P + e.p^k, y_P + r.p^k)$ . Since the curves  $E^\nu$  and  $E^{\tilde{\Sigma}}$  must be isomorphic, the equality between the corresponding  $j$ -invariants gives the third equation:

$$A_v^3.(B^{\tilde{\Sigma}})^2 - (A^{\tilde{\Sigma}})^3.B_v^2 = 0$$

After replacing in this equation  $r$  and  $p.e$  by their values, we obtain at precision  $2k$  an equation of the form:

$$\theta^{\tilde{\Sigma}} + a.\theta + b = 0.$$

that can be solved using Algorithm 2.1 to obtain  $\theta$ ,  $e$  and  $r$ . This variant is summarized in Algorithm 5.4. We note that the advantage of using all constraints at the same time, is that it automatically solve the initialisation problem (see Lemma 5.2).

**Example 5.4.** Let  $E$  be an ordinary elliptic curve over  $\mathbb{F}_5[T]/M(T)$  with  $M(T) = T^{10} + 3T^6 + 3T^5 + T^2 + 2T + 4$  given by the equation  $y^2 = x^3 + a_4x + a_6$  where :

$$a_4 = 3T^9 + 4T^7 + 3T^6 + 3T^3 + T^2 + 2T + 2 \quad \text{and} \quad a_6 = 2T^9 + T^7 + 2T^6 + 2T^3 + 4T^2 + 3T + 3;$$

its  $j$ -invariant is

$$j_0 = 2T^7 + T^6 + T^5 + 4T^3 + T^2 + 2T + 2;$$

and  $P_0 = (x_0, y_0)$  is its nonzero 5-torsion where:

$$x_0 = 2T^8 + T^7 + 3T^6 + T^3 + 2T^2 + 2T + 3 \quad \text{and} \quad y_0 = 4T^9 + T^8 + T^7 + 2T^5 + 3T^4 + T^3 + T;$$

The Teichmüller polynomial  $\tilde{M}$  of  $M$  at precision 13 is

$$\begin{aligned} \tilde{M} = & T^{10} + 759170540T^9 + 1187000135T^8 + 435927860T^7 + 1154383168T^6 + 1177330303T^5 + \\ & 512301245T^4 + 661739075T^3 + 46449971T^2 + 1140095647T + 1220703124 \end{aligned}$$

*Input* Coefficients  $(A4, A6)$  and  $p$ -torsion  $P$  at precision  $k$ .

*Output*  $\tilde{J} = J + e.p^k$  at precision  $2k - 1$ .

- Choose nonzero  $r_1$  and  $r_2$  ;
- Set  $A6_{r_1} = A6 + r_1.p^k$  and  $A6_{r_2} = A6 + r_2.p^k$  ;
- Compute the Lift of  $P_{r_1} =$  and  $P_{r_2}$  in both cases  $(A4, A6_{r_1})$   $(A4, A6_{r_2})$  ;
- Compute the  $j$ -invariants  $J_{v_{r_1}}$  and  $J_{v_{r_2}}$  of the curves  $(A4, A6_{r_1})^\nu$  and  $(A4, A6_{r_2})^\nu$  at precision  $p^{2k}$  ;
- Set  $J_{r_1} = \text{Jinvariant}(A4, A6_{r_1})$  and  $J_{r_2} = \text{Jinvariant}(A4, A6_{r_2})$  Then  $R_1 = J_{r_1} - J$  and  $R_2 = J_{r_2} - J$  at precision  $p^{2k}$  ;
- Solve the system of equations  $\begin{cases} J_{v_{r_1}} = A + B.R_1.p^{k-1} \\ J_{v_{r_2}} = A + B.R_2.p^{k-1} \end{cases}$  at precision  $p^{2k-1}$  ;
- $a = -p.(B^\Sigma)^{-1}$  and  $b = \frac{A^\Sigma - J}{p^{k-1}}.(B^\Sigma)^{-1}$  at precision  $p^k$  ;
- $e = \text{Artin-Schreier}(a, b, k)$  ;
- return  $(J + e.p^{k-1})$  at precision  $p^k$  ;

---

**Algorithm 5.3** Lifting the  $j$ -invariant by computing the Verschiebung via a point of  $p$ -torsion

---

*Input* The equation  $y^2 = x^3 + A.x + B$  of a curve  $E$  over  $\mathbb{F}_{p^n}$ , a point  $P$  of  $p$ -torsion, the precision  $m$ .

*Output* The equation  $y^2 = x^3 + \tilde{A}.x + \tilde{B}$  of the curve  $\tilde{E}$  at precision  $m$ .

- $k = 1$  ;
- While  $k \leq \lceil (m/2 + 1) \rceil$  ;
  - a. Choose the
  - b. Then  $r = \frac{1}{2y_P} [(x_P^3 + A.x_P + B - y_P^2)/p^k + (3.e.x_P^2 + A.e + \theta)]$ ;
  - c. and extract  $p.e$  from  $\Psi_p(x_P + e.p^k, A, B + \theta.p^k) = 0$
  - d. Compute using  $A_v^3.(B^\Sigma)^2 - (A^\Sigma)^3.B_v^2 = 0$  the equation  $\theta^\Sigma + a.\theta + b = 0$ .
  - e. Compute using Algorithm 2.1 the error  $\theta$  then  $e, r$ .
  - f.  $B = B + \theta.p^k$ ,  $x_P = x_P + e.p^k$ ,  $y_P = y_P + r.p^k$  and  $k = 2k$ ;
- Return  $A, B$  and  $P$  ;

---

**Algorithm 5.4** Variant to compute the canonical lift when given a point of  $p$ -torsion

---

The above method computes the lifted coefficients  $[_{A_4, A_6}]$ , the lifted  $j$ -invariant  $\mathcal{J}$  and  $p$ -torsion of  $\tilde{E}$  at precision 4:

$$\theta_1 = 214T^9 + 510T^8 + 323T^7 + 89T^6 + 59T^5 + 38T^4 + 116T^3 + 166T^2 + 68T + 600$$

$$\begin{aligned} p.e_1 &= (18\theta_1 + 13)T^9 + (18\theta_1 + 18)T^8 + (20\theta_1 + 11)T^7 + (4\theta_1 + 20)T^6 + (\theta_1 + 4)T^5 \\ &\quad + (24\theta_1 + 20)T^4 + (22\theta_1 + 10)T^3 + (9\theta_1 + 17)T^2 + (7\theta_1 + 16)T + (22\theta_1 + 11) \\ r_1 &= (5\theta_1 + 3e)T^9 + (20\theta_1 + (2e + 4))T^8 + (13\theta_1 + (5e + 18))T^7 + (19\theta_1 + (13e + 24))T^6 + (10\theta_1 + (20e + 16))T^5 \\ &\quad + (14\theta_1 + (4e + 1))T^4 + (6\theta_1 + (18e + 19))T^3 + (11\theta_1 + (14e + 20))T^2 + (\theta_1 + (23e + 12))T + (8\theta_1 + (4e + 11)) \end{aligned}$$

$$\begin{aligned} e_1 &= T^9 + 2T^8 + 3T^7 + T^6 + 4T^5 + 4T^3 + T^2 + 4T + 3 \\ r_1 &= 9T^9 + 23T^8 + 10T^7 + 10T^6 + 9T^5 + 23T^3 + 15T^2 + 10T + 12 \end{aligned}$$

**Acknowledgements.** We thank Djiby SOW (FST-UCAD-Senegal) for his comments and suggestion on earlier version of this paper. We are supported by the FAST project and ANR CIAO. Experiments presented in this paper were carried out using PARI/GP [PAR19].

## REFERENCES

- [BDL+20] D. Bernstein, L. De Feo, A. Leroux, and B. Smith. “Faster computation of isogenies of large prime degree”. In: (2020). URL: [arXiv:%202003.10118](https://arxiv.org/abs/202003.10118) (cit. on p. 3).
- [BMS+08] A. Bostan, F. Morain, B. Salvy, and É. Schost. “Fast algorithms for computing isogenies between elliptic curves”. In: *Math. Comp.* <inria-00091441> 73.263 (2008), pp. 1755–1778 (cit. on p. 1).
- [BS09] R. Bröker and A. Sutherland. “An explicit height bound for the classical modular polynomial”. In: *The Ramanujan Journal* (2009), pp. 1–21 (cit. on p. 2).
- [CFA+06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, eds. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xxxiv+808. ISBN: 978-1-58488-518-4; 1-58488-518-1 (cit. on p. 8).
- [Elk92] N. Elkies. “Explicit isogenies”. In: *manuscript, Boston MA* (1992) (cit. on p. 1).
- [Elk98] N. Elkies. “Elliptic and modular curves over finite fields and related computational issues”. In: *American Mathematical Society, International Press 7 of AMS/IP Studies in Advanced Mathematics* (1998). Ed. by C. P. on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin, pp. 21–76 (cit. on p. 1).
- [Eng09] A. Enge. “Computing modular polynomials in quasi-linear time”. In: *Math. Comp* 78.267 (2009), pp. 1809–1824 (cit. on p. 2).
- [Gau04] P. Gaudry. “Algorithmes de comptage de points d’une courbe définie sur un corps fini”. 2004. URL: <http://www.loria.fr/~gaudry/publis/pano.pdf> (cit. on p. 6).
- [Har07] D. Harvey. “Kedlaya’s algorithm in larger characteristic”. In: *International Mathematics Research Notices* (2007), 29 pages (cit. on p. 2).
- [Ked01a] K. Kedlaya. “Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology”. In: *Preprint* (2001). arXiv: [math/0105031](https://arxiv.org/abs/math/0105031) (cit. on p. 2).
- [KU11] K. S. Kedlaya and C. Umans. “Fast polynomial factorization and modular composition”. In: *SIAM Journal on Computing* 40.6 (2011), pp. 1767–1802 (cit. on pp. 4, 12).
- [Ked01b] K. S. Kedlaya. “Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology”. In: *J. Ramanujan Math. Soc.* 4.16 (2001), pp. 323–338 (cit. on p. 2).
- [Koh96] D. Kohel. “Endomorphism rings of elliptic curves over finite fields”. PhD thesis. 1996 (cit. on p. 5).
- [LS08] R. Lercier and T. Sirvent. “On Elkies subgroups of  $\ell$ -torsion points in elliptic curves defined over a finite field.” In: *Journal de théorie des nombres de Bordeaux* 20.3 (2008), pp. 783–797 (cit. on p. 2).
- [LST64a] J. Lubin, J.-P. Serre, and J. Tate. *Elliptic Curves and formal groups*. 1964. URL: <http://ma.utexas.edu/users/voloch/lst.html> (cit. on p. 1).
- [LST64b] J. Lubin, J. Serre, and J. Tate. “Elliptic curves and formal groups”. In: *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts* (1964) (cit. on p. 5).
- [MR20] A. Maiga and D. Robert. “Computing the canonical lift of genus 2 curves in odd characteristic”. In: (Dec. 2020). In preparation. URL: [http://www.normalesup.org/~robert/pro/publications/articles/%20canonical\\_lift\\_g2.pdf](http://www.normalesup.org/~robert/pro/publications/articles/%20canonical_lift_g2.pdf) (cit. on p. 8).

- [Mes72] W. Messing. “The crystals associated to Barsotti-Tate groups”. In: *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Springer, 1972, pp. 112–149 (cit. on p. 5).
- [Nak93] T. Nakamura. “A note on elliptic curves with ordinary reduction”. In: *Archiv der Mathematik* 60.5 (1993), pp. 440–445 (cit. on p. 6).
- [PAR19] PARI Developers. *PARI/GP, version 2.12.1*. available from <http://pari.math.u-bordeaux.fr/>. The PARI Group. 2019 (cit. on pp. 9, 18).
- [R] H. R. “Asymptotically optimal p-adic point-counting, e-mail to NMBRTHRY list, December”. In: () (cit. on pp. 1, 2).
- [Rob21a] D. Robert. “Efficient algorithms for abelian varieties and their moduli spaces”. PhD thesis. Université Bordeaux, June 2021. URL: <http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf>. Slides: <2021-06-HDR-Bordeaux.pdf> (1h, Bordeaux). (Cit. on pp. 2, 13).
- [Rob21b] D. Robert. “Efficient algorithms for abelian varieties and their moduli spaces”. In: *Habilitation à diriger les recherches* (Mar. 2021). URL: <http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf> (cit. on p. 3).
- [Sat00a] T. Satoh. “The canonical lift of an ordinary elliptic curve over a finite field and its point counting”. In: *J. Ramanujan Math. Soc* (2000), 15:247–270 (cit. on pp. 1, 8, 11, 12).
- [Sat00b] T. Satoh. “The canonical lift of an ordinary elliptic curve over a finite field and its point counting”. In: *J. Ramanujan Math. Soc.* 15.4 (2000), pp. 247–270 (cit. on pp. 1, 8, 11, 14).
- [Sch85] R. Schoof. “Elliptic curves over finite fields and the computation of square roots mod  $p$ ”. In: *Mathematics of computation* 44.170 (1985), pp. 483–494 (cit. on p. 1).
- [Sil86] J. H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate Texts in Mathematics. Corrected reprint of the 1986 original. New York: Springer-Verlag, 1986, pp. xii+400. ISBN: 0-387-96203-4 (cit. on p. 11).
- [Skj03] B. Skjernaas. “Satoh’s algorithm in characteristic 2”. In: *Math. Comp.* 72(241) (2003), 477–487(electronic) (cit. on p. 7).
- [Tat97] J. Tate. “Finite flat group schemes”. In: *Modular forms and Fermat’s last theorem*. Springer, 1997, pp. 121–154 (cit. on p. 11).
- [Vél71] J. Vélou. “Isogénies entre courbes elliptiques”. In: *Compte Rendu Académie Sciences Paris Série A-B* 273 (1971), A238–A241 (cit. on p. 4).
- [Ver03] F. Vercauteren. “Computing zeta functions of curves over finite fields”. In: *PhD thesis, Katholieke Universiteit Leuven* (2003) (cit. on pp. 1, 2).
- [Vil18] G. Villard. “On computing the resultant of generic bivariate polynomials”. In: *Proceedings of the 2018 acm international symposium on symbolic and algebraic computation*. 2018, pp. 391–398 (cit. on p. 13).

CHEIKH ANTA DIOP UNIVERSITY, DAKAR, SENEGAL

ÉQUIPE FAST, LIRIMA (LABORATOIRE INTERNATIONAL DE RECHERCHE EN INFORMATIQUE ET MATHÉMATIQUES APPLIQUÉES)

Email address: [abdoulaye.maiga@aims-senegal.org](mailto:abdoulaye.maiga@aims-senegal.org)

INRIA BORDEAUX-SUD-OUEST, 200 AVENUE DE LA VIEILLE TOUR, 33405 TALENCE CEDEX FRANCE

Email address: [damien.robert@inria.fr](mailto:damien.robert@inria.fr)

URL: <http://www.normalesup.org/~robert/>

INSTITUT DE MATHÉMATIQUES DE BORDEAUX, 351 COURS DE LA LIBÉRATION, 33405 TALENCE CEDEX FRANCE

ÉQUIPE FAST, LIRIMA (LABORATOIRE INTERNATIONAL DE RECHERCHE EN INFORMATIQUE ET MATHÉMATIQUES APPLIQUÉES)