Towards computing canonical lifts of ordinary elliptic curves in medium characteristic

ABDOULAYE MAIGA AND DAMIEN ROBERT

Abstract. Let p be a prime; using modular polynomial Φ_p, Satoh et al [Sat00; Ver03; Gau04] 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 complexity $\tilde{O}(nm)$ Bit operations 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 $\tilde{O}(\sqrt{p}nm)$ when we are provided a rational point of p-torsion on the curve. This allows to extend Saoth's point counting algorithm to larger p.
Keywords: 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 method [Sch85] gives 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 ℓ-adic étale cohomology: if $\chi(t)$ is the characteristic polynomial of the Frobenius π_q, $\chi(t) \mod \ell$ is computed modulo several primes ℓ by looking at the action of π_q on (a subgroup of) the ℓ-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 $\chi \mod \ell$ in $\tilde{O}\left((\ell + \log q)\ell \log q\right)$, hence reconstruct χ in $\tilde{O}\left(\log^4 q\right)$.

In 2000, a second class of algorithms was introduced by Satoh [Sat00], 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 $\mathbb{Q}_q = \mathrm{Frac}(\mathbb{Z}_q)$ the unique unramified extension of $\mathbb{Q}_p$ of degree n. Then [LST64a] establishes the existence of a unique (up to isomorphisms) elliptic curve $E^{\uparrow}$ over $\mathbb{Z}_q$ for every ordinary elliptic curves $E/\mathbb{F}_q$ such that the modulo p reduction of $E^{\uparrow}$ is E and $\mathrm{End}(E^{\uparrow}) \cong \mathrm{End}(E)$ as a ring. The curve $E^{\uparrow}$ 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 $\tilde{O}_p(n^2)$.

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; Gau04] proceed in four steps:

2010 *Mathematics Subject Classification.* Primary .

Key words and phrases. canonical lift, point counting.

We thank the FAST team and CIAO ANR Project.

(1) Compute the canonical lift $E^{\uparrow}/\mathbb{Z}_q$ at p-adic precision m by solving the equation:
$$\Phi_p(j(E^{\uparrow}), \Sigma(j(E^{\uparrow}))) = 0$$
via a Newton lift. Here j is the j-invariant, Φ_p the modular polynomial classifying p-isogenies, and Σ the (small) Frobenius on $\mathbb{Z}_q$.

(2) Lift the kernel $E[p]_{\mathrm{et}}$ of the Verschiebung to $E^{\uparrow}$ via a Newton lifts. The kernel of the Verschiebung modulo p is defined by the x-coordinates of its points: $H_p(x) = \prod_{P \in E[p]_{\mathrm{et}} \setminus 0_E}(x - x(P))$, and its lift $\tilde{H}_p$ is the unique étale lift dividing the p-division polynomial $\Psi_p(E^{\uparrow})$.

(3) Compute the isogeny $E^{\uparrow} \to E^{\uparrow}/\tilde{H}_p$ using Vélu's formula, and an isomorphism u between $E^{\uparrow}/\tilde{H}$ and $\hat{\Sigma}(E^{\uparrow})$. Since Vélu's isogenies are normalised, applying Σ to this isomorphism u gives (up to a sign) the action λ_0 of $\hat{\pi}^{\uparrow}$ on the tangent spaces dx/y and $\Sigma(dx/y)$ of $E^{\uparrow}$ and $E^{\uparrow\sigma}$.

(4) Compute the norm $\lambda = N_{\mathbb{Q}_q/\mathbb{F}_q}(\lambda_0)$. This recovers the inversible eigenvalue of the big Frobenius π_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 $m \geqslant (n+5)/2$, 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 $h(\Phi_p) \leqslant 6p \log p + 18p$ (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 Φ_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 constrast, 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 [Rob21, § 5.3.8] to evaluate Φ_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 χ with complexity in time (and space) of $O_p(n^{3+\epsilon})$. Havey 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 $\tilde{O}(\sqrt{p} n^{5/2} m + n^4 m \log p)$ (at the cost of a worse dependency on n).

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 [Rob21]) 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 [Rob21, Chapter 6] a new approach of Satoh's method which works by only using the modular polynomial

Φ_p to both lift the curve and the isogeny. This allows to dispense with the computation of the division polynomial Ψ_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 [Rob21, Remark 6.6.2], assuming a point of p-torsion is given on E.

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

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 $E^{\uparrow}/\mathbb{Z}_q$ 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 χ_π 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 Φ_p and the division polynomial Ψ_p in Satoh's algorithm by directly evaluating isogenies (ie solving the equation $j(E^\nu) = j(E^{\hat{\Sigma}})$ where E^ν 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 $E'/ < P >$ 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 $E/\pm 1 \mapsto (E/ < P >)/\pm 1$.

Using Vélu's formula, we have $I(p, m, \mathbb{Z}_q) = \tilde{O}(pm \log q) = \tilde{O}(pmn)$. A recent improvement of Vélu's formula [**DeFoeBernstein**] 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 $e \leqslant p - 1$ (which we can compute using Hasse's formula), and to find one of them require computing a root of the division polynomial Ψ_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 $\tilde{O}(p \log^2 q + \sqrt{p} me \log q) = \tilde{O}(pn^2 + \sqrt{p} men)$. (If χ_π is already known the complexity becomes $\tilde{O}(\log^2(q^e) + \sqrt{p} me \log q) = \tilde{O}(e^2 n^2 + \sqrt{p} men)$.)*

In the worst case, $e = O(p)$ so the complexity is $\tilde{O}(p \log^2 p + p^{3/2} m \log q) = \tilde{O}(pn^2 + p^{3/2} mn)$ is not better than Theorem 1.1. In the best cases, when $e = O(\log p)$; for instance if the trace $t = 1 \bmod p$ (which implies $e = 1$); the complexity is $\tilde{O}(p \log^2 q + p^{1/2} m \log q) = \tilde{O}(pn^2 + p^{1/2} mn)$. 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 $n \geqslant 1$.
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 Σ that reduces to the (small) Frobenius automorphism σ on the residue field $\mathbb{F}_q$. The large Frobenius (and its lift) will be denoted by σ_q and Σ_q respectively, and sometime we will denote σ by σ_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 Σ 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 $\overline{M}(X)$ of degree n over $\mathbb{F}_p$, this allows for a fast computation of Σ without invoking modular composition.

We recall the Frobenius σ induces an isogeny $\pi : E \rightarrow E^{\sigma}, P \mapsto P^{\sigma}$, and σ_q induces an endomorphism π_q. The Verschiebung $\hat{\pi} : E \rightarrow E^{\hat{\sigma}}$ is the dual of $\pi : E^{\hat{\sigma}} \rightarrow E$ (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 $\pi^{\uparrow}$ and $\hat{\pi}^{\uparrow}$. In this article, we always denote $E^{\uparrow}$ the canonical lift of E, while $\tilde{E}$ will denote a candidate lift (which may or may not be canonical).

In odd characteristic any elliptic curve will be represented by its reduced Weierstrass equation denoted $y^2 = x^3 + a_2x^2 + a_6$ or $y^2 = x^3 + a_4x + a_6$ depending on the characteristic p of the base the field is 3 or greater.

2. Background

Let $E/\Bbbk$ be an elliptic curve, and Ψ_ℓ its polynomial of ℓ-torsion (or ℓ-division polynomial) associated with the equation of the curve. A point $P = (x, y)$ on E is a point of ℓ-torsion if and only if its coordinates constitute a solution of Ψ_ℓ.
An isogeny ϕ is a non trivial morphism between elliptic curves which is also a group morphism. The multiplication morphism is identified with $\mathbb{Z}$ then $\mathbb{Z} \subset \mathrm{End}(E)$. Furthermore when the base field $\Bbbk$ is $\mathbb{F}_q$ we have: $\mathbb{Z}[\pi_q] \subset \mathrm{End}(E)$ where π_q is the Frobenius endomorphism. In the case where E is ordinary: $\chi(X) = X^2 - tX + q$ is the characteristic polynomial of π_q where t is the trace of π_q and verifies the relation $|t| \leqslant 2\sqrt{q}$ called Hasse's bound. Therefore, if we set $D_{\pi_q} = t^2 - 4q < 0$ then : $\#E(\Bbbk) = q + 1 - t$ and $\mathbb{Z}[\pi_q] \subset \mathrm{End}(E) \subset \mathcal{O}_{\mathbb{K}}$ where $\mathbb{K} = \mathbb{Q}[\sqrt{D_{\pi_q}}]$.

2.1. **Vélu's Algorithm.** According to the inputs, the algorithms for calculating isogenies can be classified into two large groups. The first ones initiated by Vélu [Vél71] takes an elliptic curve E and a subgroup K of E then outputs an explicit form of isogeny $\phi : E \longrightarrow E/K$ and an equation of E/K. Then for every $P \in E$:

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

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 $char(\mathbb{k}) > 3$ 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 ϕ of degree ℓ with domain E Set:

$$Q(x) = \gcd(f(x), h(x))$$

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

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

$$\phi(x, y) = (\alpha(x), y\alpha(x))$$

$$\text{where} \quad \alpha(x) = \ell x - d_1x - (3x^2 + a_4).\frac{D'(x)}{D(x)} - 2f(x).\left(\frac{D'(x)}{D(x)}\right)'.$$

And E/K is given by the equation:

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

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

On the other hand, the modular polynomial Φ_ℓ encodes directly the j-invariants of ℓ-isogenous 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 $E^\uparrow$ over $\mathbb{Z}_q$ such that.*

- *E is the reduction of $E^\uparrow$ modulo p ,*
- *$End(E^\uparrow) \cong End(E)$,*

$E^\uparrow$ is called the canonical lift of E, and is also uniquely characterised by the fact that the Frobenius π_q lifts to $E^\uparrow$, or that π lifts to an isogeny $E^\uparrow \to E^{\uparrow\Sigma}$, ie by the equation

$$\Phi_p(j(E^\uparrow), j(E^\uparrow)^\Sigma)) = 0.$$

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

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

Remark 2.3. If $E^\uparrow/\mathbb{Z}_q$ is an elliptic curve, then it is the Néron model of its generic fiber $E^\uparrow_\eta$. Furthermore, by the property of Néron models, $E^\uparrow(\mathbb{Z}_q) = E^\uparrow_\eta(\mathbb{Q}_q)$. 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 $\Phi_p(j(E^{\uparrow}), j(E^{\uparrow})^{\Sigma})) = 0$.

We know that the modular polynomial satisfies the relation:

$$\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \mod p$$

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

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

Thus we deduce that the Frobenius π has multiplicity 1 and the Verschiebung $\hat{\pi}$ has multiplicity p. In fact we have over $\mathbb{Q}_q$ two points (P, Q) on $E^{\uparrow}[p]$ that reduce to $\overline{P}$ and 0 respectively. The p kernels $\langle P + kQ \rangle$ with $0 \leqslant k < p$ reduce to $\overline{P}$ (ie the kernel of the Vershiebung) and the last $\langle Q \rangle$ reduces to $\langle \mathcal{O} \rangle$ (ie the kernel of the Frobenius). So we have p isogenies on $E^{\uparrow}$ 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. □

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 Σ of $\mathbb{Q}_q$ and $j \in \mathbb{Z}_q$ is an approximation of $\tilde{j}$ at precision k i.e $\tilde{j} = j + p^k e$, for some error $e \in \mathbb{Z}_q$ that we want to find. Using the modular equation and Taylor expansion of Φ_p we have:

$$0 = \Phi_p(j + p^k e, j^{\Sigma} + p^k e^{\Sigma})$$

$$0 = \Phi_p(j, j^{\Sigma}) + p^k e \frac{\partial \Phi_p}{\partial X}(j, j^{\Sigma}) + p^k e^{\Sigma} \frac{\partial \Phi_p}{\partial Y}(j, j^{\Sigma}) + p^{2k}(...)$$

Dividing by p^k, we get

$$u + e \frac{\partial \Phi_p}{\partial X}(j, j^{\Sigma}) + e^{\Sigma} \frac{\partial \Phi_p}{\partial Y}(j, j^{\Sigma}) \equiv 0 \mod p^k.$$

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

$$e^{\Sigma} + ae + b = 0.$$

with $a \equiv 0 \mod p$ and $b \neq 0 \mod p$ called "**Artin-Schreier equation**"in [Gau04]. Set $e = x + p^k \alpha$ with $\alpha \in \mathbb{Z}_q$, the error α can be determine using algorithm 2.3 (a general case of Harley's algorithm).

Input $a, b \in \mathbb{Z}_q$ with $a \equiv 0 \mod p$ and $b \not\equiv 0 \mod p$ and the precision m.
Output e such that $e^\sigma + ae + b \equiv 0 \mod p^N$ with $a = 0 \mod p$

- ➔ If $N = 1$ Return e the unique root of $e^\sigma + b \equiv 0 \mod p$.
- ➔ $x \leftarrow \text{ArtinSchreier}(a, b, N/2)$.
- ➔ 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; using the relation between them and the lifted 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 for example a_2 or a_4 (depending on p), then the equation between the lifted j-invariant and the second parameter a_6 provides a simple Newton algorithm to lift it. Furthermore in characteristic $\geqslant 5$, Skjernaa [Skj03] has suggested to simply take $a_4 = 3\lambda$ and $a_6 = 2\lambda$ with

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

and then lift λ using the lifted j-invariant. This method is faster than the first. It needs only one inversion in $\mathbb{Z}_q$ form the lifted j-invariant.

2.5. **The division polynomial.** If $E/\Bbbk$ is an elliptic curve with a short Weierstrass equation, and $P = (x, y)$, then $\ell.P = (\frac{\xi_\ell(x)}{\psi_\ell^2(x)}, \frac{\omega_\ell(x,y)}{\psi_\ell^3(x,y)})$ where ξ_ℓ and ω_ℓ are expressible in terms of the $\psi_{\ell-2}, \psi_{\ell-1}, \psi_\ell, \psi_{\ell+1}, \psi_{\ell+2}$, and the ψ_ℓ 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 ℓ 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 ℓ is odd, and $\Psi_\ell(x) = \psi_\ell(x)/2y$ when ℓ is even. This reformulation is such that Ψ_ℓ is always in $\Bbbk[x]$ whether ℓ is even or odd. It is easy to adapt the recurrence formula to compute the Ψ_ℓ 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 Ψ_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 Ψ_p modulo $\tilde{H}_p$ a candidate lift of H_p.

We remark that we can evaluate Ψ_p modulo H simply by evaluating the recurrence relation modulo H. Also from the recurrence relation on Ψ_ℓ, we get a recurrence relation on Ψ'_ℓ, 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 π_q is inseparable, we lift the Verschiebung $\widehat{\pi}_q$ over $\mathbb{Z}_q$ by lifting its kernel.
We set $E_{n-i} = E^{\sigma^i}$ and π_i is the isogeny between E_{i+1} and E_i defined by $(x, y) \mapsto (x^\sigma, y^\sigma)$. Then the Verschiebung $\widehat{\pi}_q$ decomposes as follow:

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

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

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

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

T.Satoh introduced in [Sat00, § 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 $t = \operatorname{ord}_p(G'(x))$. Let $u \in \mathbb{N}$ be such that $G(x) \equiv q(x)h(x) \mod p^{u+t}$. Then the polynomial :

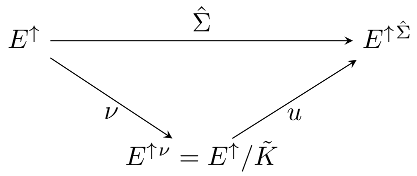
$$H(x) = h(x) + \left(\frac{G(x)}{G'(x)} h'(x) \mod h(x) \right)$$

is a lift of $h(x)$ at precision p^{2u} and $G(x) \equiv Q(x)H(x) \mod p^v$ where $v = 2u + min(t, u)$ (see [Sat00]). 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 $O(n)$.

Satoh then applies this construction to lift H_p, by [Sat00, 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 $E^\uparrow$ at sufficient precision m (given by Hasse-Weil bounds), one can evaluate the action of the Verschiebung on the differential form $\dfrac{dx}{y}$ as detailed by Satoh's diagram.



Here the isogeny ν is computed by Vélu's algorithm from the lift $H_p^\uparrow$ of the kernel of the Verschiebung.

Since the isogeny ν is normalized, the action of the isogeny $\hat{\pi}^\uparrow$ on the differential form of $E^\uparrow$ is given by the isomorphism $\pm u$ on $E^{\uparrow\nu}$; let us denote it by λ_1. Concretely, we have $\hat{\pi}^\uparrow = \pm u \circ \nu$, and if $u(x,y) = (u^2 x, u^3 y)$, $\lambda_1 = \pm u$.

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

$$E^\uparrow \longrightarrow E^{\uparrow\Sigma} \longrightarrow \cdots \longrightarrow E^{\uparrow\Sigma^{n-1}}$$

The action on the differential forms along the cycle will be given by the successive conjugates of λ_1. Finally, by composition, the action of the dual endomorphism $\hat{\pi}_q^\uparrow$ of $\pi_q^\uparrow$ on the main differential form of $\tilde{E}$ is given by the product of all these conjugates, i.e. by the norm of λ_1. On the other hand the norm of $N_{\mathbb{Q}_q/\mathbb{Q}_p}(\lambda_1)$ is simply given as the resultant of λ_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 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 $E^{\uparrow}$ at precision $m = (n+5)/2$;
- ➔ Compute the action λ_1 of an isomorphism $u : E^{\uparrow\nu} \to E^{\uparrow\hat{\Sigma}}$;
- ➔ Compute $\lambda^2 = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\lambda_1^2\right)$;
- ➔ Compute λ the correct square root from λ^2 and $t = \lambda + q/\lambda \mod q$ 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

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

Since we only have λ_1 up to a sign, taking its norm λ 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 $E^{\uparrow}/\mathbb{Z}_q$ and the lift $H_p^{\uparrow}$ 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 χ_π once we have $E^{\uparrow}$ and $H_p^{\uparrow}$ to precision m is $\tilde{O}(pn^2)$.

In the rest of this paper, we will explain how we can compute $E^{\uparrow}$ and $H_p^{\uparrow}$ 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 $E^{\uparrow\hat{\Sigma}}$ (since $\hat{\Sigma}$ is typically more expensive to compute than Σ) by applying the above method to $E^{\uparrow\Sigma}$, the canonical lift of E^{σ} 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 inversible 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

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

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 inversible 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 inversible. 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:

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

Let $J(x) = dF(x)$ be the Jacobian, and $H(x) = d^2F(x,x)$ 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:

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

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

are the vector colomns of $\frac{1}{2}H(x)$.

More generally, in N variables we may compute $d^kF(x)$ 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 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 $j(\tilde{E}) = j(E^{\uparrow}) \mod p^2$:

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

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

If these conditions are satisfied, and $\mathbb{F}_{q^e}$ is the smallest extension of $\mathbb{F}_q$ where the points of $E[p]_{\mathrm{et}}$ 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 $\tilde{E} \to E$), 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 ζ_p. Furthermore, if $P \in \tilde{E}[p](\mathbb{Z}_q^{\mathrm{ur}})$, then $\Psi'_P(P)$ is of valuation 1.

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

$$0 \to \tilde{E}^0 \to \tilde{E} \to \tilde{E}^{\mathrm{et}} \to 0.$$

This exact sequence commutes with specialisation, so since $\operatorname{Spec} \mathbb{Z}_q$ is connected, $\tilde{E}^0$ is exactly the kernel of the projection map $\tilde{E} \to E$. In particular, since $\tilde{E}^{\mathrm{et}}[p]$ is étale and $\mathbb{Z}_q$ is complete hence Henselian, it is the unique étale lift of $E[p]_{\mathrm{et}}$, and $\tilde{E}^0[p]$ is a lift of $E[p]_{\mathrm{loc}}$ which is of multiplicative type (since it is the Cartier dual of $E[p]_{\mathrm{et}}$), hence its points live in a ramified extension of $\mathbb{Z}_q$. So if $\tilde{P} \in \tilde{E}[p](\mathbb{Z}_q^{\mathrm{ur}}) \neq 0_{\tilde{E}}$, the subgroup generated by $\tilde{P}$ induces a splitting $\tilde{E}[p] = \tilde{E}^0[p] \oplus \tilde{E}^{\mathrm{et}}[p]$, in particular $\tilde{P} \notin \tilde{E}^0[p]$. This proves the equivalence of (1) and (2). The rest of the equivalences are from [Sat00, Theorem 3.1]. Furthermore we have $\tilde{E}[p](\mathbb{Z}_q^{\mathrm{ur}}) = \tilde{E}^{\mathrm{et}}[p](\mathbb{Z}_q^{\mathrm{ur}}) = \tilde{E}^{\mathrm{et}}[p](\mathbb{Z}_{q^e})$, and since $\tilde{E}^0[p]$ is the Cartier dual of $\tilde{E}^{\mathrm{et}}$ its points live in $\mathbb{Q}_q(\zeta_p)$.

Finally, $\Psi'_p(P) = 1$ by Satoh's lemma [Sat00, Lemma 3.7]. □

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 Ψ_p using the recursive formula for division polynomials to get H_p. But Ψ_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 λ, the inversible eigenvalue of the Frobenius modulo p. Then $\sigma(P) = \lambda.P$, so e is the order of λ.

There are two methods to find λ 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 Vélu's formula, and look at the action on the differentials (i.e 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 $u : E/H_p \simeq E^{\hat{\sigma}}, (x, y) \mapsto (u^2 x, u^3 y)$, so if $\phi : E \to E/H_p$ is given by Vélu'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 ϕ 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 insted, 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 $P \neq 0_E$ 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 $x_Q^3 + a_4 x_Q + a_6$ (when $p > 3$). 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 $\dfrac{\partial f}{\partial y}(P)$ non null modulo p. The Jacobian of the system is given by:

$$\begin{pmatrix} \dfrac{\partial f}{\partial x}(x,y) & \dfrac{\partial f}{\partial y}(x,y) \\ \Psi_p'(x) & 0 \end{pmatrix}$$

Then using Satoh's lemma [Sat00, Lemma 3.7], we conclude that the determinant of the Jacobian of those system at P has p-valuation 1:

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

Thus in the Newton's lifting steps, we lost 1 precision on the coordinates of $\tilde{P}$. Also to boostrap 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 Ψ_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 [MR20, Section A.3.] and [Maï22, Section 1.2]. 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 $\tilde{P} = u + p.a_1(u) + p^2.a_2(u) + \cdots$ 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_λ is the point of p-torsion with x-coordinate given by the root λ of H_p, its lift $\tilde{P}_\lambda$ is given by $\lambda + p.u_1(\lambda) + p^2.u_2(\lambda) + \cdots$.

Then $\tilde{H}_p(x)$ is given by the resultant $\mathrm{Res}_u(x - u, \tilde{P})$. 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 $\Psi_p \mod \tilde{H}_p = 0 \mod p^{2k}$ (where $2k$ is our target precision).

Indeed by Lemma 2.5, Ψ_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 $a = \Psi_p \mod \tilde{H}_p^*$ and $b = \Psi_p \mod (\tilde{H}_p^* + p^k)$. Then the derivative of our Newton process is given by $c = (b-a)/p^k$, and we solve the equation $a + cp^kQ = 0 \mod (\tilde{H}_p^*, p^{2k})$ (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 $\tilde{H}_p = \tilde{H}_p^* + p^kQ$.

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

$$\tilde{H}_p = \tilde{H}_p^* + e \quad \text{with} \quad e = \frac{\Psi_p.\tilde{H}^{*\prime}_p}{\Psi_p'} \mod \tilde{H}_p^*.$$

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 satisfies 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 ℓ 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 χ_ℓ 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 Ψ_ℓ may not be absorbed in the $\tilde{O}$ notation here).

5. Computing the Canonical Lift without using Modular Polynomials

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

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

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

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 $J^\uparrow$ of the canonical lift. We first note that Proposition 4.1 gives a convenient criteria to compute the canonical lift $E^\uparrow$ 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 $j(\tilde{E}) = j(E^\uparrow) \mod p^2$ if and only if $\Psi_{\tilde{E},p}(P) = 0$ modulo p^2, if and only if $\Psi_{\tilde{E},p} = 0$ modulo (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 $\Psi'_p(P) = 0 \mod p$. The same hold for $\Psi_{\tilde{E},p}$ modulo H_p.

By Section 4, is $\Psi_{\tilde{E},p}(P) = 0$ modulo 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 [Sat00, Theorem 3.1].

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

So $\tilde{E} \mod p^2$ corresponds to the unique elliptic curve (up to isomorphism) such that $\Psi_{\tilde{E},p}(P) = 0$. Such we look for an equation of $\tilde{E} : y^2 = \tilde{f}(x) \mod p^2$ such that $\Psi_{\tilde{E},p}(P) = 0$. Taking an arbitrary lift for the first parameter (for example a_2 or a_4), we look for $\tilde{a}_6 = a_6 + pr_1$, and we solve for r_1 by using the methods of Section 3. If we have H_p instead, we do the same computation using the equation $\Psi_{\tilde{E},p} \% H_p = 0 \mod p^2$ (as remarked in [Maï22, Page 47]).

Assume that we have J at p-adic precision $k \geqslant 2$, 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 $x = j(E)$ modulo 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 $F(x) = x^{\hat{\Sigma}}$.

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

Lemma 5.3. *Let J satisfies $F(J) = J^{\hat{\Sigma}}$ at precision $k \geqslant 2$, 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 $\Phi_p(J', F(J')) = 0$ modulo p^{2k}. Write $F(J') = F(J) + p^k e'$, then $\Phi_p(J, F(J)) + \partial\Phi_p/\partial_x(J, F(J))p^k e + \partial\Phi_p/\partial_y(J, F(J))p^k e' = 0$ modulo p^{2k}, hence $B = \partial\Phi_p/\partial_x(J, F(J))/\partial\Phi_p/\partial_y(J, F(J))$ is of valuation -1 by Kronecker's formula (see Section 2.3 and Lemma 2.4). □

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

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

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 $F(J + p^k e) = A + (Bp)p^{k-1}e = J^{\hat{\Sigma}} + e^{\hat{\Sigma}} p^k$ mod p^{2k-1}.

By applying the Frobenius Σ, we get:

$$A^{\Sigma} + B^{\Sigma}.e^{\Sigma}.p^k = J + e.p^{k+1}$$

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

$$e^{\Sigma} + a.e + b = 0 \mod p^{k+1}.$$

where $a = 0$ modulo p. We then solve this equation using algorithm Section 2.3.

This proves Theorem 1.1. The resulting algorithm is as follows, depending on whether the étale p-torsion is rational or not.

Computing the canonical lift from lifting a non-rational p-torsion. We are considering the p-torsion H_p non rational over $\mathbb{F}_q$ and we want to compute the canonical lift $E^{\uparrow}$ of $E/\mathbb{F}_q$ without taking any extension to factor H_p. In practice, we can also bypass the computation of p-th division polynômial in order to deal with lifting only coefficient instead off lifting the full polynomial (like in Satoh's lemma [Sat00, Lemma 3.7]).

Example 5.4. Let consider an elliptic curve $(E) : y^2 = x^3 + a_4 x + a_6$ over $\mathbb{F}_q = \mathbb{F}_p / < m >$ such that : $p = 43$ with $m = T^{13} + 4T + 40$, $a_4 = T^3 + T$ and $a_6 = 45 + T$;
The p-torsion is given by :
$H_p = x^{21} + (15T^{12} + 29T^{11} + 14T^9 + 17T^8 + 36T^7 + 24T^6 + 36T^5 + 26T^4 + 26T^3 + 30T + 16)x^{20} + (36T^{12} + 30T^{11} + 13T^{10} + 31T^9 + 15T^8 + 5T^7 + 24T^6 + 7T^5 + 22T^4 + 26T^3 + 21T^2 + 27T + 16)x^{19} + (17T^{12} + 4T^{11} + 17T^{10} + 41T^9 + 16T^8 + 14T^7 + 38T^5 + 42T^4 + 38T^3 + 12T^2 + 23T + 40)x^{18} + (31T^{12} + 29T^{11} + 20T^{10} + 21T^9 + 20T^8 + 2T^7 + 8T^6 + 9T^5 + 12T^4 + 30T^3 + 29T^2 + 6T + 32)x^{17} + \cdots\cdots + (19T^{12} + 8T^{11} + 36T^9 + 20T^8 + 5T^7 + T^6 + 39T^5 + 26T^4 + 4T^3 + 11T^2 + 34T + 25)x^2 + (4T^{12} + 28T^{11} + 28T^{10} + 29T^9 + 11T^8 + 11T^7 + 28T^6 + 4T^5 + 18T^4 + 25T^3 + 41T^2 + 22T + 13)x + (6T^{12} + 39T^{11} + 2T^{10} + 2T^9 + 5T^8 + 7T^7 + 42T^5 + 17T^4 + 22T^3 + 7T + 27)$;
The teichmuler polynomials of m is M:
$M = T^{13} + 114384547890216406603135684T^{12} + 889671371522715305250283 66T^{11} + 126406081376404358544543410T^{10} + 70522505892296739689 0094603T^9 + 123490241010463260981288680T^8 + 286366816713660400219 52538T^7 + 447603824491746333370784 59T^6 + 702853200254050286806043 83T^5 + 117572780660116767368899264T^4 + 990944423300178633317192 18T^3 + 928127117885798577990014 18T^2 + 886445901878565636354633 86T + 829753675415987559372117 42$;

At the initialization step we get at precision 2 :
$a_6^{\uparrow} = 1075T^{12} + 1462T^{11} + 86T^{10} + 1462T^9 + 1419T^8 + 1591T^7 + 1333T^6 + 989T^4 + 301T^3 + 473T^2 + 44T + 1206$
$H_p^{\uparrow} = x^{21} + (1649T^{12} + 889T^{11} + 301T^{10} + 1132T^9 + 318T^8 + 853T^7 + 282T^6 + 1498T^5 + 284T^4 + 1101T^3 + 731T^2 + 890T + 489)x^{20} + (1670T^{12} + 632T^{11} + 744T^{10} + 1794T^9 + 1778T^8 + 5T^7 + 970T^6 + 953T^5 + 409T^4 + 757T^3 + 795T^2 + 70T + 1478)x^{19} + (1608T^{12} + 90T^{11} + 1135T^{10} + 557T^9 + 274T^8 + 315T^7 + 946T^6 + 597T^5 + 816T^4 + 253T^3 + 485T^2 + 883T + 685)x^{18} + (504T^{12} + 674T^{11} + 1439T^{10} + 1354T^9 + 966T^8 + 2T^7 + 180T^6 + 525T^5 + 571T^4 + 1535T^3 + 545T^2 + 1167T + 1838)x^{17} + \cdots\cdots + (1094T^{12} + 223T^{11} + 1154T^9 + 1697T^8 + 650T^7 + 517T^6 + 512T^5 + 1144T^4 + 1337T^3 + 871T^2 + 163T + 713)x^2 + (1638T^{12} + 286T^{11} + 716T^{10} + 1190T^9 + 183T^8 + 527T^7 + 544T^6 + 47T^5 + 835T^4 + 971T^3 + 1847T^2 + 22T + 271)x + (565T^{12} + 1415T^{11} + 389T^{10} + 1206T^9 + 478T^8 + 1512T^7 + 1118T^6 + 343T^5 + 1135T^4 + 1140T^3 + 1333T^2 + 265T + 1145)$
At precision 5
$a_6^{\uparrow} = 89370641 * T^12 + 31831997 * T^11 + 88053164 * T^10 + 131452419 * T^9 + 34842126 * T^8 + 69363128 * T^7 + 117235329 * T^6 + 50131937 * T^5 + 73112298 * T^4 + 130025679 * T^3 + 137852668 * T^2 + 74788396 * T + 128867261$
$H_p^{\uparrow} = x^21 + (13554174 * T^12 + 36600038 * T^11 + 64815104 * T^10 + 67687647 * T^9 + 59582451 * T^8 + 134006827 * T^7 + 49244011 * T^6 + 118940100 * T^5 + 2516945 * T^4 + 46906060 * T^3 + 69650669 * T^2 + 124782289 * T + 47939684) * x^20 + (90938500 * T^12 + 88285953 * T^11 + 6661186 * T^10 + 146103281 * T^9 + 55222808 * T^8 + 55217423 * T^7 + 146968778 * T^6 + 18353912 * T^5 + 33075536 * T^4 + 77858707 * T^3 + 51544852 * T^2 + 13709545 * T + 109684846) * x^19 + \ldots\ldots\cdots + (123394582T^{12} + 51380192T^{11} + 136676618T^{10} + 100271263T^9 + 1787057T^8 + 131033604T^7 + 118802895T^6 + 93268845T^5 + 76848465T^4 + 38498549T^3 + 57899855T^2 + 56771386T + 56131494)x^2 + (34498474T^{12} + 78144530T^{11} + 105348953T^{10} + 32496161T^9 + 106847830T^8 + 135578968T^7 + 66380160T^6 + 55349948T^5 + 47217372T^4 + 50491786T^3 + 123934340T^2 + 127599985T + 100834884)x + (97736340T^{12} + 19082364T^{11} + 129429400T^{10} + 70719178T^9 +$

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 $E^{\uparrow}$ at precision 2 using the equation $\Psi_p^{\uparrow} \mod H_p = 0$ at precision 2 ;
- ➔ Compute $H_p^{\uparrow} \mod p^2$.
- ➔ $k = 1$
- ➔ while $k < \lceil (m+1)/2 \rceil$;
  - *a.* Compute at precision $2k$ two lifts $\tilde{E}_{r_1} = (a_4, A6_{r_1})$ and $\tilde{E}_{r_2} = (a_4, A6_{r_2})$ of the curve $E^{\uparrow}$;
  - *b.* Compute $\tilde{H}_p \mod p^{2k+1}$ on these two curves using Section 4.4.
  - *c.* Compute the j-invariants Jv_{r1} and Jv_{r2} of the curves $(\tilde{E}_{r_1})^{\nu}$ and $(\tilde{E}_{r_2})^{\nu}$ at precision p^{2k} ;
  - *d.* Set J_{r1} =Jinvariant$(\tilde{E}_{r_1})$ and J_{r2} =Jinvariant$(\tilde{E}_{r_2})$
    Then $R_1 = J_{r1} - J$ and $R_2 = J_{r2} - J$ at precision p^{2k} ;
  - *e.* Solve the system of equations $\begin{cases} \mathrm{Jv}_{r1} = & A + B.R_1.p^{k-1} \\ \mathrm{Jv}_{r2} = & A + B.R_2.p^{k-1} \end{cases}$ at precision p^{2k-1} ;
  - *f.* $a = -p.\left(B^{\Sigma}\right)^{-1}$ and $b = \dfrac{A^{\Sigma} - J}{p^{k-1}}.\left(B^{\Sigma}\right)^{-1}$ at precision p^{k+1} ;
  - *g.* e =Artin-Schreier(a, b, k) ;
  - *h.* $J = J + e.p^{k-1}$ at precision p^{2k-1};
  - *i.* Compute the correct coefficient $a_6^{\uparrow}$ of $E^{\uparrow}$;
  - *j.* $k = 2k - 1$;
- ➔ Return $E^{\uparrow}$ at precision m .

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

---

$98744474T^8 + 51160676T^7 + 106856462T^6 + 69941993T^5 + 106515661T^4 + 86377734T^3 + 41992682T^2 + 119635682T + 34063380)$
We get sufficient precision at precision 9 to extract the invertible eigenvalue of the Frobenius :

$$\chi(X) = X^2 - 18505011142X + 171826412428229078524 3$$

Then the cardinality of $E/\mathbb{F}_q$ is given by $\chi(1)$:

$$\#E(\mathbb{F}_q) = 171826412426378577410 2$$

Input Coefficients (a_4, a_6), p-torsion P and integer m the precision.
Output Coefficients $(a_4^{\uparrow}, a_6^{\uparrow})$ at precision m.

- ➔ $k = 1$;
- ➔ Use Initialization Phase (Lemma 5.2) to compute $E^{\uparrow} = (a_4, a_6^{\uparrow})$ and $J^{\uparrow}$ at precision 2;
- ➔ While $(2 \leqslant k \leqslant (m+1)/2)$;
  - *a.* Choose r_1 and r_2 and set $A6_{r_1} = a_6^{\uparrow} + r_1.p^k$ and $A6_{r_2} = a_6^{\uparrow} + r_2.p^k$;
  - *b.* Compute the lift of P_{r_i} on the curve $(a_4^{\uparrow}, A6_{r_i})$ using Lemma 4.4 and equation $(p'+1)P = -p'.P$ for $i = 1, 2$;
  - *c.* Compute the j-invariants Jv_{r_i} of the curves $(a_4^{\uparrow}, A6_{r_i})^{\nu}$ at precision p^{2k} for $i = 1, 2$;
  - *d.* Set J_{r_i} =Jinvariant$(a_4^{\uparrow}, A6_{r_i})$ then $R_i = J_{r_i} - J$ at precision p^{2k} for $i = 1, 2$;
  - *e.* Solve the system of equations $\begin{cases} \mathrm{Jv}_{r1} = & A + B.R_1.p^{k-1} \\ \mathrm{Jv}_{r2} = & A + B.R_2.p^{k-1} \end{cases}$ at precision p^{2k-1} ;
  - *f.* $a = -p.\left(B^{\Sigma}\right)^{-1}$ and $b = \dfrac{A^{\Sigma} - J}{p^{k-1}}.\left(B^{\Sigma}\right)^{-1}$ at precision p^{k+1} ;
  - *g.* e =Artin-Schreier(a, b, k) ;
  - *h.* $J = J + e.p^{k-1}$ at precision p^{2k-1};
  - *i.* Compute the lift $(a_4^{\uparrow}, a_6^{\uparrow})$ of coefficients at $2k-1$ using $J^{\uparrow}$ and the method Section 2.4 ;
  - *j.* $k = 2k - 1$;
- ➔ Return $(a_4^{\uparrow}, a_6^{\uparrow})$.

Algorithm 5.2 Computing the canonical lift via a rational p-torsion point .

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 Algorithm 5.2.

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 $\tilde{E}$.

Example 5.5. Let consider an elliptic curve $(E) : y^2 = x^3 + a_4x + a_6$ over $\mathbb{F}_q = \mathbb{F}_p / < m >$ such that :
$p = 211$;
$m = t^{15} + 8t^{14} + 206t^{13} + 49t^{12} + 45t^{11} + 55t^{10} + 32t^9 + 96t^8 + 189t^7 + 95t^6 + 9t^5 + 177t^4 + 16t^3 + 97t^2 + 81t + 1$;
$a_4 = 110t^{14} + 100t^{13} + 192t^{12} + 200t^{11} + 154t^{10} + 165t^9 + 160t^8 + 33t^7 + 175t^6 + 180t^5 + 39t^4 + 67t^3 + 26t^2 + 100t + 201$
and $a_6 = 7$;
Set P a p-torsion on $E/\mathbb{F}_q$ defined by :
$x_P = 209t^{14} + 191t^{13} + 50t^{12} + 39t^{11} + 12t^{10} + 67t^9 + 175t^8 + 56t^7 + 143t^6 + 8t^5 + 21t^4 + 120t^3 + 195t^2 + 208t + 143$,
$y_P = 92t^{14} + 175t^{13} + 200t^{12} + 8t^{11} + 126t^{10} + 210t^9 + 163t^8 + 196t^7 + 71t^6 + 150t^5 + 132t^4 + 80t^3 + 174t^2 + 22t + 65$;
$M = t^{15} + 5014573003526249771092844833030631692t^{14} + 2508250673811790198356701590783305 05t^{13} + 12461860950267527063067749557738448867t^{12} + 13351281210916388766618807255497055379t^{11} + 14574297177749812777165744835955759876t^{10} + 13968172740626834170042958704238035034t^9 + 11959193518517769133846943903751712396t^8 + 14080772563481554246350833862901058192t^7 + 4329361002368013574474146544749055085t^6 + 3600448955644966285034050267654638135t^5 + 10859183703290584349715258254689167500t^4 + 13790189976030233374534232493116985 69t^3 + 15384382802016088362543219242389550854t^2 + 13866543145981282254887307294428271201t + 1$;
Set $\tilde{a}_6$ a lift of a_6, then the p-torsion P can be lifted using the revisiting Newton's method on the affine equation: $F(P) = 0$ where $F(P) = \begin{cases} x_P^3 + a_4x_P + \tilde{a}_6 - y_P^2 \\ x_{210P} - x_P \end{cases}$ is defined with $[210]P = -P$. We can use the binary decomposition $210 = 2(2^3(2^2(2^2+1)+1)+1)$. At the initialization step we get at precision 2 :
$a_4^{\uparrow} = 20155t^{14} + 24787t^{13} + 23402t^{12} + 42189t^{11} + 37079t^{10} + 17045t^9 + 38984t^8 + 4464t^7 + 11147t^6 + 31830t^5 + 8268t^4 + 42267t^3 + 8677t^2 + 38924t + 2944$;
$x_{P^{\uparrow}} = 8649t^{14} + 36905t^{13} + 15453t^{12} + 33588t^{11} + 27864t^{10} + 12516t^9 + 43008t^8 + 43100t^7 + 28417t^6 + 18787t^5 + 11837t^4 + 22486t^3 + 38597t^2 + 8015t + 41921$,
$y_{P^{\uparrow}} = 35540t^{14} + 40054t^{13} + 24043t^{12} + 44107t^{11} + 37262t^{10} + 37979t^9 + 22107t^8 + 20452t^7 + 28345t^6 + 2260t^5 + 24186t^4 + 13584t^3 + 12623t^2 + 15847t + 17578$,
Hence we get at precision 12
$a_4^{\uparrow} = 2671718397668446896245970571t^{14} + 7060110570574242483425506768t^{13} + 1863467057625922197202091330t^{12} + 7578341423072727332831284825t^{11} + 1225584654390802694047832384t^{10} + 4288054694853384905571233211t^9 + 4394063442273828854164622 19t^8 + 9806988187226526283476173 93t^7 +$

$17003240429345653747913895 75t^6+4159936551553945984408369135t^5+5744396478240046766966965230t^4+4001643821057362004394876054t^3+$
$3873451890089346457847128654t^2 + 1394628609546236807464828 77t + 4968440206433640486316965944,$
$x_{P\uparrow} = 4446916850782394358861409451t^{14}+4330220999418990698699272696t^{13}+5308979423975087666818733490t^{12}+3705566609929340947479439845t^{11}+$
$6223359622880788382339154388t^{10}+2132250830138068751534690002t^9+4857610651598985078850902892t^8+7063120582039236210401691172t^7+$
$4389340046238299658479497034t^6+1701146282179561848855628863t^5+1012321137697066878509823253t^4+5340655651549791715821694921t^3+$
$3777597162001370872110467946t^2 + 7001961475794151633283686228t + 1435755778615985441497624964,$
$y_{P\uparrow} = 2477305725884587529844928487t^{14}+6894409214265980087849247 85t^{13}+4467264683540606352595210873t^{12}+2758217319636590617986800899t^{11}+$
$1007676165174401824911354 40t^{10}+6494765071129798930344648655t^9+1576910752234224180897967589t^8+6745328242851815254809112088t^7+$
$3143851716850320603234935821t^6+1560608638027421125966158938t^5+6150931329336162774631347274t^4+7666601798563957936348691372t^3+$
$6218874202007780879605860308t^2 + 3975286049416045993013712520t + 1519162756670746362559746819,$

This precision is sufficient to extract the invertible eigenvalue of the Frobenius :

$$\chi(X) = X^2 + 450017538940817098X + 7315378969765317844042040186933865 1$$

Then the cardinality of $E/\mathbb{F}_q$ is given by $\chi(1)$:

$$\#E(\mathbb{F}_q) = 731537896976531788904379408101557 50$$

Acknowledgements. We thank Djiby SOW (FST-UCAD-Senegal) for his comments and suggestion on ealier 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

[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 pp. 1, 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 (cit. on p. 2).

[Ked01b] K. 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).

[KU11] K. 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).

[Koh96] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. 1996 (cit. on p. 4).

[LS08] R. Lercier and T. Sirvent. "On Elkies subgroups of ℓ-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).

[Maï22] A. Maïga. "Relèvement Canonique de Surfaces Abéliennes". Theses. EDMI - Université Cheikh Anta Diop - Sénégal, June 2022. URL: https://hal.science/tel-04210605/file/ClassicThesis.pdf (cit. on pp. 13, 14).

[MR20] A. Maïga and D. Robert. "Computing the canonical lift of genus 2 curves in odd characteristic". In: (Dec. 2020). Preprint. URL: http://www.normalesup.org/~robert/pro/publications/articles/%20canonical_lift_g2.pdf (cit. on pp. 8, 13).

[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).

[Rob21] 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, 3).

[Sat00] 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, 12, 14, 15).

[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. 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. Skjernaa. "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. Vélu. "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 p. 1).

[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

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
Email address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE

Équipe FAST, LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées)