Computing the Canonical Lift of Genus 2 Curves in Odd Characteristics

Damien Robert, Abdoulaye Maiga

Computing the Canonical Lift of Genus 2 Curves in Odd Characteristics

ABDOULAYE MAIGA AND DAMIEN ROBERT

Abstract. Let $A/\mathbb{F}_q$ be an ordinary abelian surface. We explain how to use the Siegel modular polynomials, and if available the Hilbert modular polynomials to compute the canonical lift of A. As an application, if $q = p^n$, we show how to use the canonical lift to count the number of points on A in quasi-quadratic time $\tilde{O}(n^2)$, this is a direct extension of Satoh's original algorithm for elliptic curves.
We give a detailed description with the necessary optimizations for an efficient implementation.

Key words: Abelian variety, Arithmetic invariants of genus 2 curves, Modular polynomials, Canonical lift, Point counting.

1. Introduction

Let $A_0/\mathbb{F}_q$ be an ordinary abelian variety, and let $\mathbb{Z}_q = W(\mathbb{F}_q)$ be the ring of Witt vectors over $\mathbb{F}_q$. Then by a standard corollary of *Serre-Tate* theorem[LST64], there is a canonical lift $A/\mathbb{Z}_q$ of $A_0/\mathbb{F}_q$ characterised by the fact than $\mathrm{End}(A) \cong \mathrm{End}(A_0)$.

In dimension 1, this result was already shown by Deuring. Further when we denote by Σ the Frobenius substitution in $\mathbb{Q}_q/\mathbb{Q}_p$, the j-invariant of the canonical lift $\tilde{E}$ of an ordinary elliptic curve E satisfies: $\Phi_p(j, j^{\Sigma}) = 0$, where Φ_p is the level p modular polynomial. Thus using a suitable Newton methods one can recover the j-invariants of $\tilde{E}$ from $j \mod p$. This standard p-adic method was first applied by T.Satoh [Sat00] for points counting on elliptic curves over a field of small characteristic.

Since level p modular polynomial were not computed in higher dimension, the generalisations of Satoh's idea used instead modular equations coming from higher level theta constants. First in characteristic $p = 2$, J-F.Mestre's extend the AGM method using Riemann duplication formulas for complex analytic theta functions, then for level $p > 2$ [CL08] used generalised p-multiplication formula. In another direction, Kedlaya and al. [Ked01] developed a method to compute the action of the lifted formal Frobenius on the Monsky-Washnitzer (and Dwork) cohomology groups.

However in the case of dimension 2, classical modular polynomials have been recently computed [Mil15; Mil14; MD20]: the modular polynomials Φ_p then consist in a triple of three polynomials that parametrizes Igusa modular invariants of p-isogenous abelian surfaces. In this work, we explain how to use these modular polynomials to compute the canonical lift of an abelian surface and do point counting. Like in the elliptic curve case, the algorithm proceeds in three steps:

(1) Use the modular polynomials to compute the (modular invariants) of the canonical lift;
(2) Compute the (unique) unramified lift of the kernel of the Verschibung
(3) Compute the isogeny associated to this kernel to recover the action of the Verschiebung on the tangent space, hence the two inversible eigenvalues of the Frobenius (recall that our base abelian surface is assumed to be ordinary).

Date: January 5, 2022.
2010 *Mathematics Subject Classification.* Primary 14K99, Secondary 14K10, 11G10, 11T71.
Key words and phrases. canonical lift, point counting.
We thank the FAST team and CIAO ANR Project.

Compared to the elliptic curve cases, there are small difficulties in dimension 2. First, for Step 1 we use a Newton iteration. A crucial property of modular polynomials in dimension 1, that guarantees the convergence of the Newton method, is the Kronecker relation: $\Phi_p(X,Y) \cong (X^p - Y)(Y^p - X) \pmod{()p}$. This guarantee that $\partial\Phi_p/\partial X\Phi_p(j, j^\Sigma) \cong 0 \pmod p$ and $\partial\Phi_p/\partial Y\Phi_p(j, j^\Sigma)$ is inversible modulo p. We will call these condition the Kronecker's condition.

We first show that these conditions are true in any dimension, by using Serre-Tate's local moduli. A slight technical difficulty is that this argument works for the fine moduli space, not the coarse moduli space $\mathfrak{A}_{g,\Gamma_0(p)}$. Already for elliptic curve Satoh's algorithm requires that $j(E) \notin \mathbb{F}_{p^2}$ for the Newton method to work. Furthermore, in dimension 2 the modular polynomials Φ_p only describe a scheme birational to the coarse space $\mathfrak{A}_{g,\Gamma_0(p)}$. In particular, using the modular polynomials Φ_p will only work for a dense open of abelian surfaces, we give some criterions in Section 3 for an abelian surface to be in this set.

Main Theorem 1 *Let J be the tuple of absolute invariants of a polarized abelian surface $\mathcal{A}$ over $\mathbb{F}_q$. If J satisfies the Kronecker's condition then the algorithm 3.1 computes the absolute invariants of the canonical lift of $\mathcal{A}$ over $\mathbb{Z}_q$ to precision n in $O(n^2)$ operations (here p is assumed to be constant).*

We also extend this theorem to the case of Hilbert modular polynomials, which have been computed for higher level than the Siegel ones (since they are smaller).

For Step 2, Satoh's algorithm directly lift the equation of the kernel. In dimension 2, the kernel and the p-torsion are naturally described by multivariate polynomials, so to lift it directly would require to compute a univariate representation. For this we could apply [GS12b]. In this paper we also explain how to directly lift generators of the kernel (after taking a suitable extension where the generators live). The only difficulty is that the Jacobian of the system has p-adic valuation 1, so we need to bootstrap to p-adic precision 3 before applying Newton's algorithm.

Finally Step 3 is computed using the isogeny algorithm developed in [LR12; CR10], from which we recover the action of the Verschiebung on the tangent space associated to $\tilde{\mathcal{A}}$.

We thus get:

Main Theorem 2 *(p-torsion lifting) Let $\mathcal{A}$ be an abelian surface over $\mathbb{F}_q$ satisfying the Kronecker condition, we can compute the characteristic polynomial of the Frobenius χ_p in $O(n^2)$ operations.*

Although we focus on the dimension 2 case because we only have modular polynomials for these, all our algorithms using the theta model of level 2 or 4 would be valid in arbitrary dimension, provided we had the corresponding modular polynomials.

A specificity of the dimension 2 case is that indecomposable abelian surfaces are the Jacobian of an hyperelliptic curve of genus 2: $A = \mathrm{Jac}(C)$. When computing the canonical lift of A, we explain how to lift the curve C too (from which it is easy to reconver all possible lifts). Since all (vectorial) modular functions induce a rational covariant on the curve C, and covariants are generated by the coefficients of the curve, this allows to compute lifts of modular functions.

As mentioned, in [CL08] proposed a method which relies on the computation of arithmetic invariants of canonical lifts using the coordinate system provided by the theta null points of level np^2 with $n = 2, 4$. By comparison our method only rely on rational modular invariants, or because they are convenient theta null points of level $n = 2, 4$. We should mention that, as alluded to in [LR20], one can modify the algorithm of [CL08] to use theta null points of level np, and these thete null points can be constructed from the theta null of level n along with the points of p-torsion (which we use anyway when lifting the Verschiebung). The main interest of our method is that we are able to stay on the base field, and furthermore that we can use the Hilbert modular polynomials when possible, which are much smaller.

This paper is organized as follow. At the beginning in section 2 we recall some basic fact about the both moduli spaces $\mathrm{SL}_4(\mathbb{Z})\backslash\mathfrak{H}_2$ and $\mathrm{SL}_2(\mathcal{O}_K)\backslash\mathfrak{H}_1^2$, and the general definition of Siegel and

Hilbert modular polynomials in dimension 2. In the section 3 we give a proof of the *Kronecker condition in dimension 2*; and in the both moduli, we propose a variant of Harley's algorithm using these *Kronecker condition*. In section 4, we propose an algorithm to lift a p-torsion of abelian varieties of dimension g over $\mathbb{Z}_q$ and this method is based on a property that generalizes Satoh's Lemma 3.7. in [Sat00] for abelian varieties. The section 5 concerns applications of computing canonical lift of abelian variety and we propose a quasi-linear point counting method on the Jacobians of ordinary hyperelliptic curves of genus 2 over finite fields.

The Appendix contain further results: how to lift the curve equation, the proof of the general Kronecker condition on the fine moduli space (in any dimension g), and a generalisation (well known to the experts but that we put there for completude) on the extension of Newton's algorithm to the multivariate case in the particular case that the root modulo p has multiplicities.

1.1. **Notation and Convention.** In the following we consider p a prime and $q = p^n$ with $n \geqslant 1$. Given $\mathbb{F}_q$ by $\mathbb{F}_p[X]/m(X)$ where $m(X)$ is a monic irreducible polynomial over $\mathbb{F}_p$ then $\mathbb{Q}_q$ can be represented by $\mathbb{Q}_p[X]/M(X)$ with M monic irreducible polynomial over $\mathbb{Z}_p[X]$ such that $M(X) = m(X) \mod p$. The complexity of an elementary operation over $\mathbb{Z}/p^k\mathbb{Z}[X]/M(X)$ requires $\tilde{\mathrm{O}}(nk \log p)$ with Kronecker-Schönhage method.
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 p^{th}-power Frobenius automorphism σ on the residue field $\mathbb{F}_q$.
To obtain an efficient Frobenius substitution Σ one takes m as sparse as possible and M its Teichmuller lift polynomial. We denote by :
$\tilde{\mathcal{A}}$ the lift of any variety $\mathcal{A}$,
$\tilde{A}$ the lift of any element A of $\mathbb{F}_q$,
DF the jacobian matrix of a multivariate polynomial F,
HF the Hessian matrix of F,
$\mathbb{Z}_q^{ur}$ the unramified extension of $\mathbb{Z}_q$.

2. Modular Polynomials in Dimension 2

We briefly recall the construction of the Siegel modular polynomials and the Hilbert modular polynomials, and refer to [Mil15; Mil14; MD20] for more details.

2.1. **Siegel Modular Polynomials.** We recall, that the function field $\mathbb{C}_{\Gamma_2}$ of the moduli space $\mathfrak{A}_2 = \Gamma_2/\mathfrak{H}_2$ for principally polarized abelian varieties has dimension 3 generated by the tuples: $\mathbb{C}_{\Gamma_2} = \mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ where j_1, j_2 and j_3 (also called Streng invariants) are defined by:

$$\mathrm{j}_1 = -2^{-10}\frac{\psi_4\psi_6}{\chi_{10}}, \quad \mathrm{j}_2 = 2^{-7}\cdot 3\frac{\psi_4^2\chi_{12}}{\chi_{10}^2}, \quad \mathrm{j}_3 = 2^{-18}\frac{\psi_4}{\chi_{10}^2}.$$

(for the proof see [Igu62]).

Furthermore in characteristic different from 2 and when $\psi_4 \neq 0$, the tuple $(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ corresponds exactly to the isomorphism classes of the principal polarized abelian surfaces. However these invariants are not defined for the product of elliptic curves (vanishing points of the cups form ψ_{10}). And when $\psi_4 = 0$, the correspondence fail to specify the isomorphism class. Fortunately using the triples of invariants defined in [MR21, Theorem 2], one can describe isomorphism classes in the locus ψ_4 on $\mathfrak{A}_2$. For f a modular function, we define $f_p(\Omega) = f(\Omega/p)$. Then the function field $\mathbb{C}(\mathfrak{A}_{g,\Gamma_0(p)})$ of $\mathfrak{A}_{g,\Gamma_0(p)} = \Gamma_2/\Gamma_0(p)$ is given by $\mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3, \mathrm{j}_{p,1}, \mathrm{j}_{p,2}, \mathrm{j}_{p,3}) = \mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)[\mathrm{j}_{p,1}]$ [BL09, Lemma 4.2].

Then the modular polynomial $\phi_{1,p}$ is the minimal polynomial of $\mathrm{j}_{p,1}$ over $\mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$, and the modular polynomials $\phi_{p,2}$ and $\phi_{p,3}$ parametrizes $\mathrm{j}_{p,2}$ and $\mathrm{j}_{p,3}$ with respect to $\mathrm{j}_{p,1}$. More precisely, if $\mathcal{C}_p$ is a set of representative classes of $\Gamma_2/\Gamma_0(p)$, $\phi_{1,p}(X) = \prod_{\gamma\in\mathcal{C}_p}(X - \mathrm{j}_{p,1}^{\gamma}) \in \mathbb{Q}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)[X]$.

And for $l = 2, 3$, $\phi_{l,p}(X) = \psi_{l,p}(X)/\phi'_{1,p}(X)$ where:

$$\psi_{l,p}(X) = \sum_{\gamma \in \mathcal{C}_p} \mathfrak{j}_{l,p}^{\gamma} \prod_{\gamma' \in \mathcal{C}_p \setminus \{\gamma\}} (X - \mathfrak{j}_{1,p}^{\gamma'}) \in \mathbb{Q}(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)[X], \quad l = 2, 3.$$

The evaluation of the $\mathfrak{j}_i$'s at $\Omega \in \mathcal{H}_2$ maps the polynomials $\phi_{1,p}(X)$, $\phi_{2,p}(X)$, and $\phi_{3,p}(X)$ to polynomials in $\mathbb{C}[X]$. If x is a root over $\mathbb{C}$ of $\phi_{1,p}(\mathfrak{j}_i(\Omega), X)$, then $(x, \phi_{2,p}(x), \phi_{3,p}(x))$ are the absolute invariants of a principally polarized abelian surface (p, p)-isogenous to the abelian variety with period matrix Ω.

The modular polynomials have denominators in the $\mathfrak{j}_i$. Let $\mathcal{L}_p$ denote the locus of the principal polarized abelian surfaces that are (p, p)-isogenous to a product of elliptic curves, it is a 2-dimensional algebraic subvariety of the moduli space $\mathfrak{A}_2$ and can be parameterized by the equation an equation $L_p = 0$ for $L_p \in \mathbb{Q}[\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3]$, induced by $\chi_{10} = 0$. Then the polynomial L_p divides the denominator of the coefficients of the polynomials $\phi_{1,p}(X)$, $\psi_{1,p}(X)$ and $\psi_{2,p}(X)$.

Remark 2.1. It is not hard to extend the definition of Siegel modular polynomial for other modular invariants (not necessarily for the full congruence subgroup), in particular to theta constant of levels 2 or 4).

2.2. **Hilbert Modular Polynomials.** If an abelian surface has real multiplication by a quadratic real order $\mathcal{O}_{\mathbb{K}}$, we can also consider β-isogenies for β a totally positive element of $\mathcal{O}_{\mathbb{K}}$.

Given modular invariants $\mathfrak{i}_1, \mathfrak{i}_2$ and $\mathfrak{i}_3$ for the Hilbert (or Humbert) surface $H_1^2/\operatorname{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}})$ where

$$\operatorname{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \operatorname{SL}_2(\mathbb{K}) : \ a, b \in \mathcal{O}_{\mathbb{K}}, \ b \in (1/\sqrt{\Delta_{\mathbb{K}}}))\mathcal{O}_{\mathbb{K}} \text{ and } c \in \sqrt{\Delta_{\mathbb{K}}}\mathcal{O}_{\mathbb{K}} \right\},$$

we can define Hilbert β-modular polynomials exactly as in the Siegel case: *The polynomials* $\phi_\beta(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$ *and* $\psi_{\beta,k} = (X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$ *for* $k = 2,\ 3$ *defined as follow, are called the* β*-modular polynomials for invariants* $\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3$.

$$\phi_\beta(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3) = \prod_{\gamma \in C_\beta} \left(X - \mathfrak{i}_{1,\beta}^{\gamma}\right) \quad \text{and} \quad \psi_\beta(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3) = \sum_{\gamma \in C_\beta} \mathfrak{i}_{2,\beta}^{\gamma} \frac{\Phi_\beta(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)}{(X - \mathfrak{i}_{1,\beta}^{\gamma})}$$

-Where in non symmetric case: $\mathcal{C}_\beta$ is the set of representatives of $\dot{\Gamma} \cap \dot{\Gamma}^0(\beta) \backslash \dot{\Gamma}$ and $\dot{\Gamma}$ be a congruence subgroup such that $\dot{\Gamma}(2, 4) \subset \dot{\Gamma} \subset \operatorname{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}})$.

Let $\dot{\Gamma}^0(\beta) = \left\{ \left(\begin{smallmatrix} a & b/\sqrt{\Delta_{\mathbb{K}}} \\ c\sqrt{\Delta_{\mathbb{K}}} & d \end{smallmatrix}\right) \in \dot{\Gamma} \ : \ b \in \beta\mathcal{O}_{\mathbb{K}} \right\}$, then the Hilbert cover $\dot{\Gamma}^0(\beta) \backslash \mathfrak{H}_1^2$ parametrizes the β-isogenous principally polarised abelian surfaces with real multiplication by $\mathcal{O}_{\mathbb{K}}$, or equivalently pairs $(\mathcal{A}, K)$ where $\mathcal{A}$ has real multiplication by $\mathcal{O}_{\mathbb{K}}$ and $K \subset \mathcal{A}[\beta]$ is a kernel stable by $\mathcal{O}_{\mathbb{K}}$ and maximally isotropic for the β-Weil pairing. Then Hilbert β-modular polynomial define a variety birational to this one, in particular given $J_1 = (\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$, a β-isogenous point $J_2 = (\mathfrak{e}_1, \mathfrak{e}_2, \mathfrak{e}_3)$ on the Hilbert modular surface is characterized by $\phi_\beta(J_1, \mathfrak{e}_1) = 0$, $\mathfrak{e}_2\phi'_\beta(J_1, \mathfrak{e}_1) = \psi_{\beta,k}(J_1, \mathfrak{e}_1)$ and $\mathfrak{e}_3\phi'_\beta(J_1, \mathfrak{e}_1) = \psi_{\beta,k}(J_1, \mathfrak{e}_1)$.

Remark 2.2.

- If ℓ is prime in $\mathcal{O}_{\mathbb{K}}$, the Hilbert modular polynomials Φ_ℓ are still smaller than the Siegel one, since they parametrize ℓ-isogenies stable under the real multiplication;
- When ℓ splits as $\ell = \beta\beta^c$, the Φ_β and Φ_{β^c} modular polynomials parametrize isogenies with cyclic kernel (inside $A[\beta]$ and $A[\beta^c]$ respectively).
- In practice it can convenient to take symmetric modular invariants for the $\mathfrak{i}$. The modular polynomials we construct then parametrize both β as well as β^c isogenies.

3. Canonical Lift of Ordinary Abelian Surfaces

Like in Satoh original method (see [Sat00]) we want use the Hilbert and Siegel modular polynomials in order to compute the modular invariants of the canonical lift via a Newton method.

3.1. **In Siegel Modular Space.** Let $\tilde{\mathcal{A}}$ be an ordinary abelian surface over $\mathbb{Z}_q$, in what follows we resume how the kernel of a (p,p)-isogenies from $\tilde{\mathcal{A}}$ reduces over $\mathbb{F}_q$.

Reduction of the (p^3+p^2+p+1) isogenies on $\mathfrak{A}_2 \otimes \mathbb{F}_q$. Let's consider the points P, Q, R and S on $\mathcal{A}[p]$, with P and Q étale, R and S ramified, and R is the dual of P, and S the dual of Q for the Weil-Pairing. An isotropic kernel $\tilde{K}$ of a p-isogeny from $\tilde{\mathcal{A}}$ has three possibilities of reduction on $\mathcal{A}$:

(1) When $\tilde{K} = \langle \tilde{R}, \tilde{S} \rangle$, it reduces to $\langle 0 \rangle$ entirely and it corresponds to the kernel of the lift of the Frobenius (1 choice).
(2) In the second case we suppose that $\tilde{K}$ reduces modulo p to a cyclic group of order p. Modulo p we have $(p+1)$ cyclic groups of order p : $\langle P + bQ \rangle$ and $\langle Q \rangle$. Suppose that they reduce to $\langle P \rangle$, then $\tilde{K}$ have the form $\langle \tilde{P} + a\tilde{R} + b\tilde{S}, c\tilde{R} + d\tilde{S} \rangle$. By using the isotropic and linear conditions we get $\tilde{K} = \langle \tilde{P} + a\tilde{R}, \tilde{S} \rangle$. This case corresponds to p choices for every cyclic group of order p modulo p. And we have $(p+1)p$ lifted kernels.
(3) And in the last case, $\tilde{K}$ reduces to $\langle P, Q \rangle$, the kernel of the Verschiebung. Ihas the form $\langle \tilde{P} + a\tilde{R} + \tilde{b}S, \tilde{Q} + c\tilde{R} + d\tilde{S} \rangle$. Using the isotropic conditions on such basis we get $b = c$. Therefor we obtain p^3 kernels and according to [Sat00], only one of them is unramified: the "canonical" lift of the Verschiebung.

We get all p^3+p^2+p+1 isogenies corresponding to the roots of $\phi_{1,p}$.

Computing the lift of Invariants. We denote by Φ a 3×1 matrix which components $\Phi_{1,p}$, $\Psi_{1,p}$ and $\Psi_{1,p}$ are the polynomials (in function of the invariants of the p-isogenous entries) coming from the modular polynomials $\phi_{1,p}$, $\phi_{2,p}$ and $\phi_{3,p}$.

$$\Phi_{1,p} = (\phi_{1,p} \cdot D_1)(u, x_1, x_2, x_3)$$
$$\Psi_{2,p} = \left(\psi_{2,p} - v \cdot \phi'_{1,p}\right) \cdot D_2(x_1, x_2, x_3, u, v)$$
$$\Psi_{3,p} = \left(\psi_{3,p} - w \cdot \phi'_{1,p}\right) \cdot D_3(x_1, x_2, x_3, u, w)$$

where D_i's are the denominators of the corresponding function. We use this notation to consider only the numerators of fractional functions. From the definitions in Section 2.1, these denominators D_1, D_2 and D_3 are in function of respectively $(\mathrm{Den}(\phi_{1,p}))$, $(\phi'_{1,p}$ and $\mathrm{Den}(\psi_{2,p}))$ and $(\phi'_{1,p}$ and $\mathrm{Den}(\psi_{3,p}))$.
Let $U = (x_1, x_2, x_3)$ denotes the absolute invariants of the first variety and $V = (u, v, w)$ represents the absolute invariants of the p-isogenous varieties.

Suppose that we can compute efficiently the Frobenius automorphism σ of $\mathbb{Q}_q$ and $X \in \mathbb{Z}_q^3$ is an approximation of $\tilde{J}$ at precision p^k i.e $\tilde{J} - X = p^k e$ for some error e over $\mathbb{Z}_q$ that we want to find. Using the modular equation and Taylor expansion of Φ_p we have:

$$0 = \Phi_p(X + p^k e, X^\sigma + p^k e^\sigma) \quad \text{implies}$$
$$0 = \Phi_p(X, X^\sigma) + p^k e \frac{\partial \Phi_p}{\partial U}(X, X^\sigma) + p^k e^\sigma \frac{\partial \Phi_p}{\partial V}(X, X^\sigma) + p^{2k}(...)$$

where by $\dfrac{\partial \Phi_p}{\partial U}$ and $\dfrac{\partial \Phi_p}{\partial V}$ we mean the jacobian matrices of the vector function Φ_p respectively in direction of U and V. Letting $\Phi'_{1,p} = \dfrac{\partial \Phi_{1,p}}{\partial u}$, we have:

$$\frac{\partial \Phi_p}{\partial V} = \begin{pmatrix} \phi'_{1,p}.D_1 & 0 & 0 \\ 0 & -\phi'_{1,p}.D_2 & 0 \\ 0 & 0 & -\phi'_{1,p}.D_3 \end{pmatrix}$$

$$\frac{\partial \Phi_p}{\partial U} = \begin{pmatrix} \frac{\partial \Phi_{1,p}}{\partial x_1} & \frac{\partial \Phi_{1,p}}{\partial x_2} & \frac{\partial \Phi_{1,p}}{\partial x_3} \\ \frac{\partial \Phi_{2,p}}{\partial x_1} & \frac{\partial \Phi_{2,p}}{\partial x_2} & \frac{\partial \Phi_{2,p}}{\partial x_3} \\ \frac{\partial \Phi_{3,p}}{\partial x_1} & \frac{\partial \Phi_{3,p}}{\partial x_2} & \frac{\partial \Phi_{3,p}}{\partial x_3} \end{pmatrix}$$

We let $\mathcal{L}_p$ the set of absolute invariants J which annihilate the product $\mathrm{Den}(\phi_{1,p}) \cdot \mathrm{Den}(\psi_{2,p}) \cdot \mathrm{Den}(\psi_{3,p})$.

Proposition 3.1. *(Kronecker's condition) Let $J = (a, b, c)$ be the absolute invariants of the abelian surface $\mathcal{A}$ over $\mathbb{F}_q$. If $a \notin \mathbb{F}_{p^2}$ and $(a, b, c) \notin \mathcal{L}_p$, and the abelian surface corresponding to J has no non-trivial p^2-endomorphism, then*

i) $\frac{\partial \Phi_p}{\partial V}(J, J^\sigma)$ *is invertible;*

ii) $\frac{\partial \Phi_p}{\partial U}(J, J^\sigma) \equiv 0 \mod p$.

Proof. In general, we show in Appendix A and Proposition A.1 that the Frobenius realizes the Kronecker conditions on the locus of the ordinary points of the fine moduli space $\mathfrak{A}_{g,\Gamma_0(p)}$, hence the Kronecker condition is valid on a dense open set of points. We check that the conditions above are sufficient.

i) We have :

$$\det\left(\frac{\partial \Phi_p}{\partial V}\right) = (\phi'_{1,p})^3 \cdot D(x_1, x_2, x_3, u)$$

where the function D represents the product $D_1.D_2.D_3$ of the denominators. Remark that the parametrization given by the modular polynomials Φ_p is such that the multiplicity of the solution can be read on $\phi_{1,p}$. - When $J = (a, b, c) \notin \mathcal{L}_p$ and $J \in \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$ then $\hat{\sigma}(J) = \sigma(J) = J$. Since modulo p the Verschiebung $\hat{\sigma}$ has multiplicity p^3 then :

$$\phi'_{1,p}((a, b, c), a^p) \equiv 0 \mod p \text{ which implies } \frac{\partial \Phi_p}{\partial V}(J, J^\sigma) \notin \mathbb{Z}_q^\times.$$

- When $J \notin \mathcal{L}_p$ and $J \notin \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$, let us consider $a \notin \mathbb{F}_p$. From Section 3.1, the Frobenius σ admit a unique lift over $\mathbb{Z}_q$, so its multiplicity is 1 modulo p in the polynôme $\phi_{1,p}(x_1, x_2, x_3, X)$. Furthermore since by assumption the only p^2-endomorphism on A is $[p]$, the isogenies other than the Verschiebung have a different codomain (otherwise composing with their dual we would get a non trivial p^2-endomorphism), then :

$$\phi'_{1,p}(a, b, c, a^p) \not\equiv 0 \mod p.$$

Further $D(a, b, c, a^p)$ is nonzero modulo p, since $J \notin \mathcal{L}_p$.
Therefore we get:

$$\frac{\partial \Phi_p}{\partial V}(J, J^\sigma) \in \mathbb{Z}_q^\times.$$

ii) The assertion $\frac{\partial \Phi_p}{\partial U}(J, J^\sigma) \equiv 0 \mod p$ means each partial derivative in respectivelly x_1, x_2 and x_3 of the polynomials $\Phi_{1,p}(x_1, x_2, x_3, u)$, $\Phi_{2,p}(x_1, x_2, x_3, u, v)$ and $\Phi_{3,p}(x_1, x_2, x_3, u, w)$ vanish 0 modulo p when evaluated in $(a, b, c) \notin \mathcal{L}_p$.

Input J, integer N the precision.
Output $\tilde{J}$ the lift of J at precision N.

- ➔ If $N = 1$ then J at precision p;
- ➔ Else $N' = N/2$;
- ➔ J =GeneralHarley(J, N');
  - *a.* $G = \frac{\partial \Phi}{\partial U}(J, J^\sigma)$; $H = \frac{\partial \Phi}{\partial V}(J, J^\sigma)$; $Q = \Phi(J, J^\sigma)$;
  - *b.* $a = G.H^{-1}$, $b = Q.H^{-1}$;
  - *c.* e =ArtinSchreier(a, b, N');
  - *d.* $J = J + p^k e$;
- ➔ Return J ;

Algorithm 3.1 GeneralHarley

Firstly let us consider the polynomial $\Phi_{1,p} = \phi_{1,p} \cdot D_1$, where the reduction modulo p of the modular polynomial $\phi_{1,p}$ is

$$\phi_{1,p}(x_1, x_2, x_3, u) = \prod_{\gamma \in \mathcal{C}_p} (u - f_{1,p}^\gamma)$$

where the $f_{1,p}^\gamma$ are in function of variables x_1, x_2 and x_3.
The original variety with modular invariant (a, b, c) can be recovered from the one with invariants (a^p, b^p, c^p) via the application of the Verschiebung. From Section 3.1, there are p^3 lifts of the Verschiebung. Then we get:

$$\frac{\partial \Phi_{1,p}}{\partial x_k}(a, b, c, a^p) \equiv 0 \mod p \quad \text{for} \quad k = 1, 2, 3.$$

Therefore every partial derivative in respectivelly x_1, x_2 and x_3 of polynomials $\Phi_{1,p}$ become 0 modulo p in (J, J^p).

For the polynomials $\Phi_{2,p}(x_1, x_2, x_3, u, v)$ and $\Phi_{3,p}(x_1, x_2, x_3, u, w)$ we use the same reasoning. □

Therefor the Kronecker conditions provides the following Newton method for computing the lift of absolute invariants for ordinary points on $\mathfrak{A}_2 \otimes \mathbb{F}_q$ satisfying these conditions.

Theorem 3.2. *Let $J = (a, b, c)$ be the absolute invariants of a polarized abelian surface $\mathcal{A}$ over $\mathbb{F}_q$. If the triple (a, b, c) satisfy the Kronecker conditions then the algorithm 3.1 computes (by doubling precision) the absolute invariants of the lifting curve $\tilde{\mathcal{A}}$ over $\mathbb{Z}_q$ to precision n in time $O(n^2)$.*

Proof. Since the matrix of the polynomials satisfies the Kronecker condition Proposition 3.1, the modular equation $\Phi_p(X + p^k e, X^\sigma + p^k e^\sigma) = 0$ becomes modulo p^k:

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

This equation is called "Artin-Shreier equation" in [Gau04]. Since $A = \frac{\partial \Phi_p}{\partial Y}(J, J^\sigma)$ annihilate modulo p, Harley proposed a method to lift the unique $e = -\sqrt[p]{B}$ (see [Gau04] for the scalar case, the multivariate case works exactly the same). □

Remark 3.3. in the Siegel moduli space R.Dupont has computed modular polynomials in function of Igusa invariants [Dup06] for the level $p = 2$. E.Milio used Streng invariants to reach

levels 3 [Mil14], unfortunately we can't use these polynomials in characterstic 3, because Streng invariants does not reduce well in this characteristic. Indeed when we express the universal invariants γ_i's in function of the algebraic Streng invariants (j_1, j_2, j_3), we get that for for instance:

$$\gamma_2 = j_2^5/(192j_3^2) - j_2^3/(12j_3), \text{ and } \gamma_3 = 2j_2^2j_1/(27j_3) + j_2^5/(3456j_3^2) - j_2^3/(72j_3)$$

does not reduce well modulo 3.

Alternatively, we can use modular invariants derived from Igusa arithmetic invariants. For instance the absolute invariants $\mathfrak{d}_1 = J_2^2/J_4$, $\mathfrak{d}_2 = J_6^2/J_4^3$ and $\mathfrak{d}_3 = J_{10}^2/J_4^5$ induce an isomorphism of $\mathcal{M}_2[J_4^{-1}]$ with the standard open of $\mathbb{A}^3$ defined by $\mathfrak{d}_3^{-1}$ over $\mathbb{Z}[1/2]$ (see [MR21, Theorem 2] for more details). In [MR21, Theorem 2], we define invariants for the three sets $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$ and $\mathcal{M}_2[J_6^{-1}]$, this suffices to get invariants on all the non-singular points on $\mathcal{M}_2 \otimes \Bbbk$. Indeed, we know from [Igu60, Theorem 4] that, if $\mathrm{char}(\Bbbk) \neq 2$, the variety $\mathcal{M}_2 \otimes \Bbbk$ has one and only one singular point, which corresponds to $J_2 = J_6 = J_8 = 0$. Since $J_2J_6 = 4J_8 + J_4^2$, then at a non-singular point either we have $J_4 \neq 0$ or $J_2 \neq 0$ or $J_6 \neq 0$. Therefor one can compute the modular polynomials in function of the absolute invariants $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$ having good reduction modulo 3 using the algorithm 3.1 in [MR21, Pages:16-17].

3.2. **In Hilbert Modular Space.** Next we work on $\mathrm{SL}_2(\mathcal{O}_\mathbb{K})\backslash\mathfrak{H}_1^2$ in place of $\mathfrak{A}_2$. It provides a polynomials of smaller size with a different lifting algorithm but the basic idea remains the same.

From the definition of Hilbert modular polynomials Section 2.2, we see that when p is inert, the lifting algorithm of the invariants follows the same process like in Siegel space. Thus we focus on Hilbert cyclic modular polynomials corresponding to a split $p = \beta\overline{\beta}$. Let Φ_β, $\Phi_{\overline{\beta}}$ be the vector function defined by the modular polynomials, then the canonical lift J verify:

$$\begin{cases} \Phi_\beta(J, Y) = 0 \\ \Phi_{\overline{\beta}}(Y, J^\sigma) = 0 \end{cases}$$

where Y represents the invariants of the middle variety defined by splitting the Frobenius isogeny into a composition of two cyclic isogenies (a β-isogeny followed by a $\overline{\beta}$-isogeny).
Therefor, knowing $J \mod p$ we can solve the system over $\mathbb{F}_q$, to find Y. Furthermore we have following result.

Lemma 3.4. *Let $J \notin \mathcal{L}_\beta$ be the invariants defined a point on the Hilbert modular space without non trivial p^2-endomorphism, such that at least one component of J does not lies on $\mathbb{F}_p$ and ϕ_β is the minimal polynomial of the modular function associated to this component, then :*

- $\dfrac{\partial\Phi_\beta}{\partial V}(J, Y) \not\equiv 0 \mod p, \quad \dfrac{\partial\Phi_{\overline{\beta}}}{\partial V}(Y, J^\sigma) \not\equiv 0 \mod p$;
- *And* $\dfrac{\partial\Phi_{\overline{\beta}}}{\partial U}(Y, J^\sigma) \equiv 0 \mod p$.

Proof. The proof works the same as in Proposition 3.1. We remark that Y is uniquely defined as the quotient of A by the non étale part of $A[\beta]$. Indeed A does not have a non trivial β^2-endomorphism, otherwise it would have a non trivial p^2-endomorphism since $\mathrm{End}(A)$ is stable under the Rosatti involution. □

Suppose we know an approximation X and T of respectively of J and Y at precision p^k, then set $\tilde{J} - X = p^k e$ and $\tilde{Y} - T = p^k r$ where $e, r \in \mathbb{Z}_q$ are the errors that we want to determine using Φ_β.
Since $J^\Sigma = X^\Sigma + p^k e^\Sigma$, by using the Taylor expansion on $\Phi_\beta(X + p^k e, T + p^k r) = 0$ and

$\Phi_{\overline{\beta}}(T + p^k r, X^\Sigma + p^k e^\Sigma) = 0$ we obtain:

$$\begin{cases} 0 = & \Phi_\beta(X,T) + p^k \dfrac{\partial \Phi_\beta}{\partial U}(X,T)\cdot e + p^k \dfrac{\partial \Phi_\beta}{\partial V}(X,T)\cdot r + p^{2k}(\cdots) \\ 0 = & \Phi_{\overline{\beta}}(T,X^\Sigma) + p^k \dfrac{\partial \Phi_{\overline{\beta}}}{\partial U}(T,X^\Sigma)\cdot r + p^k \dfrac{\partial \Phi_{\overline{\beta}}}{\partial V}(T,X^\Sigma)\cdot e^\Sigma + p^{2k}(\cdots) \end{cases}$$

where the factors $(\cdots)$ behind p^{2k} are in $\mathbb{Z}_q$.
By dividing the whole system by p^k, then we get modulo p^k:

$$\begin{cases} 0 = & \dfrac{\Phi_\beta(X,T)}{p^k} + \dfrac{\partial \Phi_\beta}{\partial U}(X,T)\cdot e + \dfrac{\partial \Phi_\beta}{\partial V}(X,T)\cdot r \\ 0 = & \dfrac{\Phi_{\overline{\beta}}(T,X^\Sigma)}{p^k} + \dfrac{\partial \Phi_{\overline{\beta}}}{\partial U}(T,X^\Sigma)\cdot r + \dfrac{\partial \Phi_{\overline{\beta}}}{\partial V}(T,X^\Sigma)\cdot e^\Sigma \end{cases}$$

From the Kronecker conditions (Lemma 3.4): $\dfrac{\partial \Phi_\beta}{\partial V}(X,T)$ and $\dfrac{\partial \Phi_{\overline{\beta}}}{\partial V}(T,X^\Sigma)$ are invertible, then we have:

$$r = -\left[\frac{\partial \Phi_\beta}{\partial V}(X,T)\right]^{-1}\left(\frac{\Phi_\beta(X,T)}{p^k} + \frac{\partial \Phi_\beta}{\partial U}(X,T)\cdot e\right),$$

Therefor we obtain the system under a *Artin-Schreier equation* form:

$$e^\Sigma + Ae + B = 0$$

where we have:

$$A = -\left[\frac{\partial \Phi_{\overline{\beta}}}{\partial V}(T,X^\Sigma)\right]^{-1}.\frac{\partial \Phi_{\overline{\beta}}}{\partial U}(T,X^\Sigma).\left[\frac{\partial \Phi_\beta}{\partial V}(X,T)\right]^{-1}.\frac{\partial \Phi_\beta}{\partial U}(X,T),$$

$$B = \left[\frac{\partial \Phi_{\overline{\beta}}}{\partial V}(T,X^\Sigma)\right]^{-1}\left(\frac{\Phi_{\overline{\beta}}(T,X^\Sigma)}{p^k} - \frac{\partial \Phi_{\overline{\beta}}}{\partial U}(T,X^\Sigma).\frac{\partial \Phi_\beta}{\partial V}(X,T)^{-1}.\frac{\Phi_\beta(X,T)}{p^k}\right).$$

Since the Kronecker conditions (Lemma 3.4) imply: $\dfrac{\partial \Phi_{\overline{\beta}}}{\partial U}(T,X^\Sigma) \equiv 0 \mod p$ then $A \equiv 0 \mod p$.
Hence we obtain the error e to correct J (at precision p^{2k}) using the *ArtinSchreier* algorithm in [Gau04, § 5.3]. Then we have the following result.

Theorem 3.5. *Let $J \in \mathbb{F}_q$ (the Gundlach invariant or the pullback of theta invariants) representing a point $\mathcal{A}$ in Hilbert space such that J satisfies the Kronecker condition for Hilbert modular polynomials. Then the previous variant of Harley algorithm (Algorithm 3.2) computes the lift $\tilde{J}$ in $O(n^2)$ operations where $n = \mathrm{ord}_p\, q$.*

4. Computing the Lift of the p -Torsion Points

From now we know how to compute the lift $\tilde{J}$ of a invariants J of an ordinary abelian surfaces $\mathcal{A}$ defined over $\mathbb{F}_q$ (satisfying Kronecker condition). If we are working with theta invariant the reconstitution of the equation of $\tilde{\mathcal{A}}$ is immediate (for example see [Gau07; GL09]). On other hand when we are working with absolute invariant coming from Igusa invariants J_{2i}'s, one can construct an equation of $\tilde{\mathcal{A}}$ by using Mestre's method and $\tilde{J}$ (see Appendix A). Since Mestre's method has bad reduction in characteristics $p \leqslant 5$, in these cases we can lift the hyperelliptic model $y^2 = f(x)$ (or the one coming from the normal form of the corresponding curve see Appendix A or [MR21, § 1]).
Next we are interesting in the lift of the p-th Frobenius morphism σ. We want to compute (up to isomorphism) its dual, the Verschiebung, from the étale p-torsion of $\tilde{\mathcal{A}}$ and an algorithm for

Input J invariants representing $\mathcal{A}$, Y the solution of the $\Phi_p(J,Y)=0$ over $\mathbb{F}_q$ and a precision N.
Output $\tilde{J}$ at precision N.

- **If** $N=1$ **Return** J and Y at precision p;
- **Else** $N'=N/2$;
- $J=$Harley@Hilbert$(J,\ Y\ N')$;
  a. $A=-\left[\frac{\partial\Phi_p}{\partial V}(T,X^\Sigma)\right]^{-1}.\frac{\partial\Phi_p}{\partial U}(T,X^\Sigma).\left[\frac{\partial\Phi_p}{\partial V}(X,T)\right]^{-1}.\frac{\partial\Phi_p}{\partial U}(X,T)$;
  b. $B=\left[\frac{\partial\Phi_p}{\partial V}(T,X^\Sigma)\right]^{-1}\left(\frac{\Phi_p(T,X^\Sigma)}{p^k}-\frac{\partial\Phi_p}{\partial U}(T,X^\Sigma).\frac{\partial\Phi_p}{\partial V}(X,T)^{-1}.\frac{\Phi_p(X,T)}{p^k}\right)$;
  c. $e=$ArtinSchreier(A,B,N');
  d. $r=-\left[\frac{\partial\Phi_p}{\partial V}(X,T)\right]^{-1}\left(\frac{\Phi_p(X,T)}{p^k}+\frac{\partial\Phi_p}{\partial U}(X,T)\cdot e\right)$,
  e. $J=J+p^ke$ and $Y=Y+p^kr$ at precision p^{2k} ;
- **Return** J and Y ;

Algorithm 3.2 Harley@Hilbert

computing isogenies in dimension 2 (see [CE14; CR10]).
In this section we give a general method to lift the p-torsion points of $\mathcal{A}$ (in any dimension).

Let $\mathcal{A}$ be an abelian variety of dimension g over $\mathbb{Z}_q$. A point $P=(x_1,..,x_m)$ on $\mathcal{A}$ is a p-torsion point if and only if $[k+1].P=-[k]P$ (with $p=2k+1$). Let's denote by M_p the Jacobian matrix of the polynomial system $[k+1].P=-[k]P$ defining the p-torsion point.

For an ordinary elliptic curve E over $\mathbb{F}_q$ then , if Ψ_p is the p-division polynomial, we have: $ord_p\Psi_p'(x)=1$ for a (x,y) in $\tilde{E}[p]\cap\tilde{E}(\mathbb{Z}_q^{ur})\neq\{\mathcal{O}\}$ from [Sat00, Lemma 3.7.]. Therefore in dimension one, the determinant of the Jacobian matrix of F has valuation 1. The following proposition provide a generalization of the Satoh lemma [Sat00, Lemma 3.7.] to a system of polynomials that defines the set the p-torsion points on ordinary abelian varieties of dimension g.

Proposition 4.1. *Let $\mathcal{A}$ be an abelian variety of dimension g over $\mathbb{Z}_q$, at any point P of $\mathcal{A}$ the tangent at P of the system M_p equals p times the identity matrix.*

Proof. It follows directly from the fact the tangent of the addition map on A is given by the addition on the tangent spaces. □

Corollary 4.2. *Let $\mathcal{A}$ be the abelian variety defined by polynomials system $(f_1,\cdots f_n)$ in $\mathbb{A}^n$. At any $P\in\mathcal{A}[p]$ there exists a basis such that :*

$$\begin{pmatrix} Jac(f_1,\cdots,f_n)\\ M_p\end{pmatrix}=\begin{pmatrix}*&*\\0&p.I_g\end{pmatrix}$$

And its determinant has p-valuation g.
Where I_g is the g dimensional identity matrix.

Proof. Let P be a point in $\mathcal{A}[p]$ then the rank of $Jac(f_1,\cdots,f_n)$ is $(n-g)$. By applying the Proposition 4.1 we get the result. □

In dimension 1 the previous result is equivalent to Satoh lemma [Sat00, Lemma 3.7.]. Unfortunately in high dimension we have a polynomial system to define the p-torsion of abelian surfaces, however using the Proposition A.7 and Corollary 4.2 we get the following result.

Theorem 4.3. *(p-torsion lifting) Let $\mathcal{A}$ be a polarized abelian variety of dimension g over $\mathbb{Z}_q$, then we can compute the lift of any p-torsion points on $\mathcal{A}/\mathbb{F}_q$ to precision N in quadratic time over $\mathbb{Z}_q$.*

Proof. For the convenience we work on the Kummer surface.
Let F be a vector function of the polynomials system defined by: $P \in \mathcal{K}$ and $[k+1].P = -[k]P$ (with $p = 2k+1$). We know from the above Corollary 4.2 that the Smith Normal Form of $(DF(P))$ has following form using a matrix base change $M \cdot S \cdot N$:

$$\begin{pmatrix} * & * \\ 0 & p.I_g \end{pmatrix}$$

According to the Proposition A.7 the Newton on F at X will work like univariate Newton for each component of X. Hence for any $P = \tilde{P} \mod p$: $\mathrm{ord}_p F_i(P_i) = 1$ and $\mathrm{ord}_p F_i'(P_i) = 0$ for the $(n-g)$ first polynomials. And for the g others polynomials we get: $\mathrm{ord}_p F_i(P_i) = 2$ and $\mathrm{ord}_p F_i'(P_i) = 1$. According to the Lemma A.3 we must add the Hessian matrix $HF(P)$ to obtain more precision on g equations . So according to [Sat00] the lift of P is unique. Then the equation :

$$F(P) + p.DF(P).R + p^2/2.{}^tR.HF(P).R = 0 \mod p^3$$

has only one solution R, such that $\mathrm{ord}_p F_i(P_i) = 3$ and $\mathrm{ord}_p F_i'(P_i) = 1$ for the g polynomials. Then the univariate Newtons appearing for the next steps, are all of type Lemma A.3 with $k_i > 2e_i$ for all i. Therefor using the Proposition A.7 one can compute the unique lift of the p-torsion point at precision p^N in quadratic time over $\mathbb{Z}_q$. □

Example 4.4. Let $y^2 = x^3 + (t^2-t)x^2 + t^3 - t^2 + 1$ be the equation of the elliptic curve E over $\mathbb{F}_3[t]/(t^5+2t+1)$.
The Teichmuller polynomial of t^5+2t+1 is at precision 3^{16}
$M = t^5 + 40187187t^4 + 22623057t^3 + 28433298t^2 + 42740657t + 1.$
Using Harley algorithm, the lift of j-invariant at precision 3^{16} is
$\tilde{j} = 4184705t^4 + 21892713t^3 + 36017948t^2 + 23621781t + 31000250.$
The lifted curve $\tilde{E}$ is given by $y^2 = x^3 + Ax^2 + B$, where :
$A = t^2 + 1,\ B = 35012730t^4 + 19700410t^3 + 13577987t^2 + 12290190t + 25369066.$
A point $P = (x, y)$ is in $\tilde{E}[3]$ if and only if $[2].P = -P$ and since the two points $[2].P$ and P lie on the same line then $P \in \tilde{E}[3] \Leftrightarrow F(x, y) = 0$ and

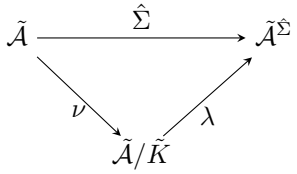
$$F(x,y) = \begin{pmatrix} -x^3 - Ax^2 + (y^2 - B) \\ 9/4x^4 + 3Ax^3 + A^2x^2 - 3y^2x - Ay^2 \end{pmatrix}.$$

Using the algorithm 4.3 at precision 3^{16} for $\tilde{P} = (2t^4 + 2t^3 + 2t^2 + 1,\ 1)$ on $E[3]$ we get:
$\tilde{P} = (555542t^4 + 15403853t^3 + 5231684t^2 + 29534907t + 30143767,\quad 11152449t^4 + 34597530t^3 + 41418387t^2 + 1833597t + 31531297).$

5. Application to Point Counting in Odd Characteristic

The previous sections details the algorithm to compute the canonical lift of abelian surfaces and theirs p-torsion groups. In this section we are interested in the main application of the the canonical lifting of genus 2 curve: *the computation of their characteristic polynomial.*
In this section we use an extension of Satoh Method in [Sat00] to evaluate the action of the Verchiebung morphism on the p-torsion group.

Let $\mathcal{C}$ be a genus 2 curve, $\mathcal{A}$ and $\mathcal{K}$ the Jacobian and the Kummer surface of $\mathcal{C}$ over $\mathbb{Z}_q$. Let Σ from $\tilde{\mathcal{A}}$ to $\tilde{\mathcal{A}}^{\Sigma}$ be the lift of the Frobenius morphism σ from $\mathcal{A}$ to $\mathcal{A}^{\sigma}$. Then $\hat{\Sigma}$ decomposes as follow :



Where ν is normalized Verschiebung computed using the Vélu's Formula and λ is an isomorphism between $\tilde{\mathcal{A}}/\tilde{K}$ and $\tilde{\mathcal{A}}^{\hat{\Sigma}}$. Since ν is normalized its action is trivial and one only need the action of the isomorphism λ to get the one of the Verchiebung $\hat{\Sigma}$.
Generally if $\pi_1, \ldots, \pi_g$ are the invertible eigenvalues of the Frobenius morphism Σ of $\tilde{\mathcal{A}}$ over $\mathbb{Z}_q$ for an ordinary abelian variety $\mathcal{A}$. Then the product $\pi_1 \cdots \pi_g$ is an element of the ring $\mathbb{Z}_q$. Since the q^{th}-power Frobenius morphism decomposes as follow :

$$\mathcal{A} \longrightarrow \mathcal{A}^{\sigma} \longrightarrow \cdots \longrightarrow \mathcal{A}^{\sigma^{n-1}}$$

We have :

$$(\pi_1 \cdots \pi_g)^k = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{\vartheta_k(\Omega^{\hat{\Sigma}})}{\vartheta_k(\Omega)}\right) = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{\vartheta_k(\Omega^{\nu})}{\vartheta_k(\Omega)}\right).$$

where ϑ_k is a modular form of weight k (equivalently a fractional covariant when $g = 2$) and $\Omega \in \mathcal{H}_g$ represents $\mathcal{A}$.

Next we describe an algorithm to compute the eigenvalues π_1 and π_2 of the Frobenius morphism on the genus 2 curve $\mathcal{C}$, further to reconstitute its characteristic polynomial in the case where its absolute invariants satisfy the Kronecker conditions.

5.1. **Description and Complexity of the Algorithm.** Since there exists a complete formulae for the conversion between Mumford and theta coordinates, for the convenience we work on the Kummer surface associated to such curve.

Initialization. Let $\mathcal{C}$ be an hyperelliptic curve of genus 2 over a finite field $\mathbb{F}_q$ of characteristic $p > 2$ such that its fundamental theta invariants given by a vector J satisfies the Kronecker conditions (Section 3 and Proposition 3.1) with a corresponding modular polynomials given for example by a vector function Φ_p. Then we have following result.

Theorem 5.1. *Our algorithm computes $\#JacC(\mathbb{F}_q)$ using in $O(M(p^4).\log(p).\log(n).n^2)$ operations using Hilbert modular polynomials and in $O(p^{15}.\log(p).\log(n).n^2)$ operations using Siegel modular polynomials.*

This algorithm is explained as follows:

Computing p-torsion over $\mathbb{F}_q$. The computation of the p-torsion over $\mathbb{F}_q$ can be done in two different ways. By solving directly the polynomials system F defined by the Kummer equation of $\mathcal{K}$ and two equations from the coordinates relations $[k+1].P = -[k]P$ (with $p = 2k+1$). On other hand the methods detailed in [GS12a] compute efficiently the p-torsion from the Mumford representation on $\mathcal{A}$ over $\mathbb{F}_q$, then we obtain the theta coordinates by conversion. Using the modular compositions in Mumford representation the computation of the p-torsion amounts to a number of operations of the form $O(pM(p^4) + p^{\omega+3})$ where ω is such that matrices of size n can be multiplied in $O(n^{\omega})$ operations. The memory requirement is $O(p^5)$ elements of $\mathbb{F}_p$. Using the group law the computation takes $O(M(p^4)\log(p))$ operations in $\mathbb{F}_p$, with a memory requirement of $O(p^4)$ elements of $\mathbb{F}_p$.

Lift Invariants. Since J satisfies the the Kronecker conditions Proposition 3.1 with corresponding vector function Φ_p of modular polynomials, the Section 3 and Algorithm 3.1 computes $\tilde{J}$. The most expensive operations resides in the evaluation of modular polynomials. Using the Hilbert modular polynomials it takes $O(p^4n^2)$ and in the case of the Siegel modular polynomials it takes $O(p^{15}n^2)$, see [Kie20]. And the resolution of Artin-Schreier algorithm costs $O(n^2 \log p)$.
One can determine the Kummer surfaces of $\tilde{\mathcal{A}}^{\Sigma}$ and $\tilde{\mathcal{A}}$ just by computing theirs equations with a formula in Appendix A in function of the lifted fundamental theta invariants.

Lift p-Torsion. Using the Theorem 4.3 one computes an approximation of the lift of any $P \in \mathcal{K}[p]$. The resolution of the system :

$$F(P) + p.DF(P).R + p^2/2.{}^tR.HF(P).R = 0 \mod p^3$$

at the beginning of the lifting can be done using a quick Gröbner basis computation. In fact this system has three trivariates polynomials of degree 2. Then the complexity this computation is negligible since it concerns only three polynomials in three variables of degree 2 , it can be done in $O(1)$. And the lift of p-torsion can be done in $O(\log n)$ times the cost of dividing two elements of $\mathbb{Z}_q$ up till precision $\Theta(n)$.

Computing the Product $\pi_1\pi_2$. We recall, for every modular invariant ϑ_k of weight k that:

$$(\pi_1\pi_2)^k = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{\vartheta_k(\tilde{\mathcal{A}}^{\hat{\Sigma}})}{\vartheta_k(\tilde{\mathcal{A}})}\right)$$

Since K is isomorphic to $\frac{1}{p}\mathbb{Z}^2/\mathbb{Z}^2$ let denote by $(\tilde{e}_1, \tilde{e}_2)$ the canonical basis that reduces to the coordinates basis (e_1, e_2) of K. The method detailed in [CR10, § 4] computes the theta null point of $\mathcal{A}/K$ knowing $(\theta_k^{\mathcal{A}}(\tilde{e}_i))_{k\in Z(n)}$ up to an unknown projective factors λ_i for $i = 1, 2$.
Let's denote by C_0 the product $\theta_0^{\mathcal{B}}(0)^r$ given by the formulae in [CR10, Prop 4.1], Then the modular invariant ϑ_k of weight k evaluated at $\Omega_{\mathcal{B}}$ is given by :

$$\vartheta_k(\Omega_{\mathcal{B}}) = \vartheta'_k(\Omega_{\mathcal{B}}) \cdot C_0^{-2(r-1)k/r}$$

From an input $\{e_1, e_2\}$ given in theta coordinates of a maximal isotropic subgroup $K \subset \mathcal{A}[\ell]$, the above algorithm outputs $\theta_k^{\mathcal{B}}(0) \times C_0$, where $C_0 = \theta_0^{\mathcal{B}}(0)$ if $\ell \equiv 1 \mod 4$ and $C_0 = \theta_0^{\mathcal{B}}(0)^3$ if $\ell \equiv 3 \mod 4$.
Let (a, b, c, d) be the level 2 thetas given by this isogeny's computation algorithm [CR10, Prop 4.1].

- In the case where $\ell \equiv 3 \mod 4$:

  $$a = \theta_0^{\mathcal{B}}(0) \cdot C_0, \cdots, d = \theta_3^{\mathcal{B}}(0) \cdot C_0$$

  where $a = \theta_k^{\mathcal{B}}(0)^4$ i.e $C_0 = \theta_k^{\mathcal{B}}(0)^3$. Since the algorithm outputs h'_4 with factor C_0^8 and $C_0^8 = a^6$, then we obtain $h_4 = h'_4/a^6$ and using a similar process $h_{10} = h'_{10}/a^{15}$.
- In the case where $\ell \equiv 3 \mod 4$ we have :

  $$a = \theta_0^{\mathcal{B}}(0) \cdot C_0, \cdots, d = \theta_3^{\mathcal{B}}(0) \cdot C_0$$

  where $C_0 = \theta_0^{\mathcal{B}}(0)$. Then $h_4 = h'_4/a^4$ and $h_{10} = h'_{10}/a^{10}$.

Let $O(N^\mu)$ and $T_{n,N}$ for fixed p, be respectively the cost of the modular multiplication and the multiplication of two polynomials of degree less than n in $(\mathbb{Z}/p^N\mathbb{Z})[X]$ modulo M up to precision N.
The norm computation phase can be done using Satoh-Skjernaa-Taguchi analytic method in [SST03] with the complexity $O(T_{n,N+\sqrt{N}} \cdot \sqrt{N})$. When the base field admits a Gaussian Normal Basis H.Y.Kim and al. introduce an algorithm to compute such norm in $O(\sqrt{N})$ time complexity and $O(nN)$ of memory at precision p^N. On other hand Harley proposed in [R] a method based

on a resultant computation using a variant of D.Mœnck GCD algorithm [RT] to compute norm $N_{\mathbb{Q}_q/\mathbb{Q}_p}$ modulo p^N in time $O\left((nN)^\mu \log n\right)$.

Computing the Characteristic Polynomial of the Frobenius. Let χ be characteristic polynomial of $\mathcal{C}$, then $\#\operatorname{Jac} C(\mathbb{F}_q) = \chi(1)$ and it is bounds by the following inequality called Hasse-Weil bound : $\lceil\left(\sqrt{q}-1\right)^2\rceil \leqslant \chi(1) \leqslant \lfloor\left(\sqrt{q}+1\right)^2\rfloor$. The symmetric polynomial of $\mathcal{C}$ denoted P_{sym} is the unitary degree 2 polynomial over $\mathbb{Z}$ whose roots are $\pi_1\overline{\pi}_1 + \pi_2\overline{\pi}_2$ and $\pi_1\pi_2 + \overline{\pi}_1\overline{\pi}_2$. And following [Rit03; CL08] one can use the LLL algorithm to recover P_{sym} knowing the $\pi_1\pi_2$. Using a quick algorithm in [Rit03], $\chi(\pm X)$ is deduced from the knowledge of P_{sym} when this one is irreducible.
However according to [Mes02] one can determine directly $\#\operatorname{Jac} C(\mathbb{F}_q)$ and $\#C(\mathbb{F}_q)$ from the knowledge of $u = \pi_1\pi_2$. Indeed $(\pi_1 + \overline{\pi}_1)$ and $(\pi_2 + \overline{\pi}_2)$ are roots of the quadratic polynomial : $X^2 - bX + a$ where : the sum of the roots $b \equiv u \mod q$ and their product a satisfies $a^2 \equiv (\lambda+2)u \mod q$ with $\lambda = (b-u)/q$, $|b| \leqslant 4q$ and $|a| \leqslant 4\sqrt{q}$. And

$$\#\operatorname{Jac} C(\mathbb{F}_q) = \prod_{i=1}^{2}(1-\pi_i)(1-\overline{\pi}_i)$$
$$\#\mathcal{C}(\mathbb{F}_q) = q + 1 - (\pi_1 + \overline{\pi}_1) - (\pi_2 + \overline{\pi}_2)$$

Computing the theta null point of the abelian variety $\mathcal{B} = \mathcal{A}/\mathcal{K}$ is doing in $O(p^r)$ operations. Using the resultant method, the norm $N_{\mathbb{Q}_q/\mathbb{Q}_p}$ can be computed in $O(n^\mu log n)$ where $\mu = 1+\epsilon$ (for n large) and $\mu = \log_2(3)$ using the FFT multiplication algorithm and the Karatsuba algorithm respectively [CFA+06] . And $\#JacC(\mathbb{F}_q)$ can be computed from $\pi_1\pi_2$ at the cost $O(n^\mu \log p)$ of a computing square over $\mathbb{F}_q$.

5.2. **Implementation.** For the following experience, we use the Siegel modular polynomials (in function of absolute level 2 theta invariants) computed using https://members.loria.fr/EMilio/modular-polynomials/.
Let

$$\begin{aligned}\mathcal{C} : y^2 = x^5 &+ (2T^8 + T^2 + T)x^4 + (T^8 + T^7 + T^6 + T^5 + T^3 + 2T + 2)x^3\\ &+ (T^9 + 2T^8 + T^6 + T^5 + T^4 + 2T^3 + 2)x^2\\ &+ (2T^9 + T^8 + 2T^7 + T^6 + T^5 + 2T^4 + 2T^2 + 1)x\end{aligned}$$

be a genus 2 curves over $\mathbb{F}_3[T]/m$ with $m = T^{10} + 2T^6 + 2T^5 + 2T^4 + T + 2$ which absolute level 2 theta invariants are given by the vector $J = (a, b, c)$

$$\begin{aligned}a =& 2T^9 + 2T^6 + 2T^5 + 2T^4 + T^3 + T^2 + T,\\ b =& 2T^9 + T^8 + 2T^7 + T^6 + T^5 + 2T^4 + 2T^2,\\ c =& 2T^9 + 2T^6 + T^4 + 2T^3 + 2T + 2\end{aligned}$$

After the lift phase, we get at precision 3^{20}:

$$\begin{aligned}M =& T^{10} + 2549079126T^9 + 1424896413T^8 + 387776124T^7 + 1501830083T^6 + 2399043737T^5\\ &+ 1835343671T^4 + 3327249759T^3 + 1052748765T^2 + 1815623119T + 3486784400\end{aligned}$$

$$\begin{aligned}\tilde{a} =& 1632442511T^9 + 31847655518T^8 + 3476194941T^7 + 3108882704T^6 + 2423383142T^5\\ &+ 1764926933T^4 + 1098986671T^3 + 2957646787T^2 + 1669307941T + 2686192050,\end{aligned}$$

$$\begin{aligned}\tilde{b} =& 18554646665T^9 + 458606629T^8 + 1644296153T^7 + 2202845860T^6 + 2959176835T^5\\ &+ 2200438487T^4 + 1716586968T^3 + 1038290165T^2 + 133634418T + 2980506843,\end{aligned}$$

$$\begin{aligned}\tilde{c} =& 3067405283T^9 + 2017143027T^8 + 1539671400T^7 + 2805617504T^6 + 754015086T^5\\ &+ 1269571459T^4 + 2964123128T^3 + 609859068T^2 + 3096552740T + 605100932,\end{aligned}$$

One can use an implementation in http://avisogenies.gforge.inria.fr of the method in [CR10, § 4], to compute the theta invariants of the p-isogenous abelian surfaces $\tilde{\mathcal{A}}/\tilde{K}$. And we obtain:

$$[1665426634T^9 + 2291786881T^8 + 319244275T^7 + 9089656527T^6 + 373529527T^5 + 3459234302T^4 + 637296308T^3 + 1615339023T^2 + 71993550T + 2412291147,$$
$$137569385T^9 + 1781159471T^8 + 2975497017T^7 + 2625983267T^6 + 3456313825T^5 + 258917388T^4 + 169437654T^3 + 2862222480T^2 + 3191428894T + 828753903,$$
$$933603536T^9 + 1711410927T^8 + 130528953T^7 + 3466168598T^6 + 1834982298T^5 + 1734316195T^4 + 2194380317T^3 + 1333319670T^2 + 2564003393T + 1123362129,$$
$$899185444T^9 + 2638232402T^8 + 1147310541T^7 + 2100019531T^6 + 2732363852T^5 + 2339070819T^4 + 1863357600T^3 + 2399257487T^2 + 1456953946T + 2821097391]$$

$$u = \pi_1\pi_2 = 2255204904638089156.$$

And we get the characteristic polynomial : $\chi(X) = X^4 - 404X^3 + 158902X^2 - 404 \cdot 3^{10}X + 3^{20}$.

Acknowledgements. We thank Xavier Caruso for his comments on an early version of this work. We are supported by the FAST project and ANR CIAO. Experiments presented in this paper were carried out using PARI/GP [PAR19] and a Magma package called AVIsogenies in http://avisogenies.gforge.inria.fr implemented by Damien Robert and Gaetan Bisson . The modular polynomials were computed using https://members.loria.fr/EMilio/modular-polynomials/.

References

[BL09] R. Bröker and . Lauter. "Modular polynomials for genus 2". In: *LMS Journal of Computation and Mathematics,* 1.12 (2009), pp. 326–339 (cit. on p. 3).

[CL08] R. Carls and D. Lubicz. "A p-adic quasi-quadratic time and quadratic space point counting algorithm". In: *International Mathematics Research Notices* (2008) (cit. on pp. 1, 2, 14).

[CN90] C.-L. Chai and P. Norman. "Bad Reduction of the Siegel Moduli Scheme of Genus Two with $\Gamma_0(p)$-Level Structure". In: *American Journal of Mathematics* 112.06 (Dec. 1990), pp. 1003–1071. URL: http://www.jstor.org/stable/2374734 (cit. on pp. 17–19).

[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. 14).

[CR10] R. Cosset and D. Robert. "Computing (ℓ, ℓ)-Isogenies in Polynomial Time on Jacobian of Genus 2 Curves". In: *American Mathematical Society* (2010), S 0025-5718(XX)0000– (cit. on pp. 2, 10, 13, 15).

[CE14] J.-M. Couveignes and T. Ezome. "Computing functions on Jacobians and their quotients". In: (2014). arXiv: 1409.0481 (cit. on p. 10).

[Dup06] R. Dupont. "Moyenne arithmetico-geometrique, suites de Borchardt et applications". PhD thesis. 2006 (cit. on p. 7).

[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. 7, 9).

[Gau07] P. Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 9).

[GL09] P. Gaudry and D. Lubicz. "The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines". In: *Finite Fields and Their Applications* 15.2 (2009), pp. 246–260 (cit. on p. 9).

[GS12a] P. Gaudry and É. Schost. "Genus 2 point counting over prime fields". In: *Journal of Symbolic Computation* (2012), 47 (4), pp.368–400. (Cit. on p. 12).

[GS12b] P. Gaudry and É. Schost. "Genus 2 point counting over prime fields". In: *Journal of Symbolic Computation* 47.4 (2012), pp. 368–400 (cit. on p. 2).

[Igu60] J.-I. Igusa. "Arithmetic Variety of Moduli for Genus Two". In: *Annals of Mathematics* Vol.72, No.3 (1960), pp. 612–649 (cit. on p. 8).

[Igu62] J. Igusa. "On Siegel modular forms of genus 2". In: *Johns Hopkins University Press* (1962), 84(1) (cit. on p. 3).

[Ked01] K. Kedlaya. "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology". In: *Preprint* (2001). arXiv: math/0105031 (cit. on p. 1).

[Kie20] J. Kieffer. "Degree and height estimates for modular equations on PEL Shimura varieties". In: (2020). arXiv: 2001.04138 [math.AG] (cit. on p. 13).

[LR12] D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". In: *Compositio Mathematica* 148.5 (Sept. 2012), pp. 1483–1515 (cit. on p. 2).

[LR20] D. Lubicz and D. Robert. "Linear representation of endomorphisms of Kummer varieties". Dec. 2020. URL: http://www.normalesup.org/~robert/pro/publications/articles/action.pdf. In preparation. (Cit. on p. 2).

[LST64] 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. 1).

[MR21] A. Maiga and D. Robert. "Computing 2-Adic Canonical Lift of Genus 2 Curves". In: *7th International Conference on Mathematics and Computing, Mar 2021, Shibpur/Virtual* (2021). URL: https://hal.inria.fr/hal-03119147 (cit. on pp. 3, 8, 9, 17).

[Mes02] J.-F. Mestre. *Notes of a talk given at the Cryptography Seminar Rennes*. 2002. URL: http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps (cit. on p. 14).

[Mil15] E. Milio. "Calcul de polynômes modulaires en dimension 2". PhD thesis. Dec. 2015. URL: https://members.loria.fr/EMilio (cit. on pp. 1, 3).

[MD20] E. Milio and R. D. "Modular polynomials on Hilbert surfaces". In: *Journal of Number Theory* 216 (2020), pp. 403–459. ISSN: 0022-314X. URL: http://www.sciencedirect.com/science/article/pii/S0022314X20301402 (cit. on pp. 1, 3).

[Mil14] E. Milio. "A quasi-linear algorithm for computing modular polynomials in dimension 2". In: *arXiv preprint arXiv:1411.0409* (2014) (cit. on pp. 1, 3, 8).

[NO80] P. Norman and F. Oort. "Moduli of Abelian Varieties". In: *Annals of Mathematics* 112.02 (Sept. 1980), pp. 413–439. URL: https://www.jstor.org/stable/1971152 (cit. on p. 17).

[PAR19] PARI Developers. *PARI/GP, version*2.12.1. available from http://pari.math.u-bordeaux.fr/. The PARI Group. 2019 (cit. on p. 15).

[Qin93] L. Qing. "Courbes Stables de genre 2 et leur schéma de modules". In: *Mathematische Annalen Springer-Verlag, 295, 201-222* (1993) (cit. on p. 20).

[R] H. R. "Asymptotically optimal p-adic point-counting, e-mail to NMBRTHRY list, December". In: () (cit. on p. 13).

[RT] M. R.T. "Fast computation of GCDs, Proceedings of the 5th Annual ACM Sym". In: () (cit. on p. 14).

[Rit03] C. Ritzenthaler. "Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis". PhD thesis. Université Denis Diderot Paris VII, June 2003 (cit. on p. 14).

[Sat00] 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, 3, 5, 10, 11, 20, 21).

[SST03] T. Satoh, B. Skjernaa, and Y. Taguchi. "Fast computation of canonical lifts of elliptic curves and its application to point counting". In: (2003), pp. 89–101 (cit. on p. 13).

Appendix A. Appendix

A.1. Reconstitution of the Lifted Genus 2 Curves Equation.

When $p > 5$. In this case Mestre's conic has good reduction. We lift the hyperelliptic model $y^2 = f(x)$ of a genus 2 curve $\mathcal{C}$ knowing the invariants of its canonical lift, as follow:
• First we construct the cubic $\mathcal{M}$ and the conic $\mathcal{L}$ of the canonical lift of $\mathcal{C}$ over $\mathbb{Z}_q$ using $\tilde{J}$.
• Since $\mathcal{M}$ and $\mathcal{L}$ have good reduction, we extract the parameterization point P of $\mathcal{M}$ mod p corresponding to the equation $y^2 = f(x)$.
• Then we lift P using $\mathcal{M}$ to $\tilde{P}$ and reconstitute the equation $y^2 = \tilde{f}(x)$ of the curve $\tilde{\mathcal{C}}$.

When $p = 3$ ou 5. In this case, Mestre's algorithm has bad reduction modulo p. When the invariants are in function of J_{2i}'s one can lift the Normal Form equation a the genus 2 curve. Indeed these invariants admit expression in term of the coefficients of Normal Form equation, then we lift these coefficients using the lift of the invariants as detailed in [MR21, §4].
For instance when we are working in characteristic 3 with invariants $\mathfrak{d}_1 = J_2^2/J_4$, $\mathfrak{d}_2 = J_6^2/J_4^3$ and $\mathfrak{d}_3 = J_{10}^2/J_4^5$ for $\mathcal{M}_2[J_4^{-1}] \otimes \Bbbk$.Let a, b, c, and d be the coefficients of the normal form equation of a genus 2 curves $\mathcal{C}$. We can write $y^2 + (1 + ax + bx^2)y = -x^3(c + dx + x^2)$ a hyperelliptic model of $\mathcal{C}$. The coefficients $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, and $\tilde{d}$ of the normal form of the curve $\tilde{\mathcal{C}}$ that reduce to $\mathcal{C}$ satisfy the following system of equations in the variables $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, and $\tilde{d}$:

$$\begin{cases} \tilde{J}_2^2 - \tilde{J}_4\tilde{\mathfrak{d}_1} &= 0, \\ \tilde{J}_6^2 - \tilde{J}_4^3\tilde{\mathfrak{d}_2} &= 0, \\ \tilde{J}_{10}^2 - \tilde{J}_4^5\tilde{\mathfrak{d}_3} &= 0 \end{cases} \tag{1}$$

where $(\tilde{\mathfrak{d}_1}, \tilde{\mathfrak{d}_2}, \tilde{\mathfrak{d}_3})$ are the lift of $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$ given by the algorithm 3.1 with modular polynomials in function of $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$. By applying the Newton method of the Section 4 and Proposition A.7 to the equation above, one compute the coefficients $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, and $\tilde{d}$ at precision N in $\tilde{O}(N)$.

A.2. Kronecker Conditions on the Siegel Ordinary Locus of $\Gamma_0(p)$-Level Structure.

In this section our goal is to give a proof to a Kronecker condition in the fine moduli space of the ordinary locus of Siegel moduli of $\Gamma_0(p)$-Level Structure. We will refer to notion in [CN90; NO80]. Let $\mathfrak{A}_{g,\Gamma_0(p)}$ be the algebraic stack such that for any scheme S, $\mathfrak{A}_{g,\Gamma_0(p)}(S)$ is the category of isogenies

$$\begin{array}{ccc} A_1 & \xrightarrow{\phi} & A_2 \\ & \searrow \swarrow & \\ & S & \end{array}$$

of principally polarized abelian schemes $(A_{i/S}, \lambda_{A_i})$, $i = 1, 2$ such that $\phi^*(\lambda_{A_2})$ defined by $\hat{\phi} \circ \lambda_{A_2} \circ \phi$ coincides to $p \cdot \lambda_{A_1}$. The moduli $\mathfrak{A}_{g,\Gamma_0(p)}$ was deeply study by P.Norman and Ching-Li Chai as scheme over $\mathbb{Z}_p$ (for more details see [CN90]). The ordinary locus $\mathfrak{A}^0_{g,\Gamma_0(p)}$ of $\mathfrak{A}_{g,\Gamma_0(p)}$ is smooth over $\mathbb{Z}_p$.

Let's suppose for the following that $\Bbbk$ is algebrailly closed with characteristic $p > 0$.
When $A_{/\Bbbk}$ is an ordinary abelian variety, the Tate module of A and its dual are given by:

$$T_pA(\Bbbk) = \lim_{\leftarrow} A[p^n](\Bbbk), \quad T_p\hat{A}(\Bbbk) = \lim_{\leftarrow} \hat{A}[p^n](\Bbbk)$$

Let S be a scheme such that p is locally nilpotent in $\mathcal{O}_S$. Let $\mathcal{I} \subset \mathcal{O}_S$ be a nilpotent ideal. $S_0 = \operatorname{Spec} \mathcal{O}/\mathcal{I}$, $A_0 \longrightarrow S_0$ be an abelian scheme. Then the general Serre-Tate Theorem state that: the functor

$$\left\{ \begin{array}{c} A \to S \text{ abelian scheme} \\ \text{with an isom } A \times_S S_0 \to A_0 \end{array} \right\} \rightsquigarrow \left\{ \begin{array}{c} G \to S \text{ a Barrozetti-Tate group} \\ \text{with an isom } G \times_S S_0 \to A_0[p^\infty] \end{array} \right\}$$

is an equivalence of category.
From the [CN90, Theorem Pages:12-13], the Serre-Tate Theorem implies that: for every geometric point $(\phi : A_{/\Bbbk} \longrightarrow B_{/\Bbbk}, \lambda_A, \lambda_B)$ of the ordinary locus $\mathfrak{A}^0_{g,\Gamma_0(p)}$ with $\phi^*(\lambda_B) = p \cdot \lambda_A$. the isogeny ϕ induice two $\mathbb{Z}_p$-linear maps: $F : V = T_pA(\Bbbk) \longrightarrow W = T_pB(\Bbbk)$ and $T : W \longrightarrow V$ (using the dual isogeny $\hat{\phi}$) such that $T \circ F = p \cdot \mathrm{id}_V$ and $F \circ T = p \cdot \mathrm{id}_W$ and further the Dieudonné contravariant functor $\hat{\mathfrak{M}}$ is canonical identified with the functor:

$$R \longmapsto \left\{ \begin{array}{c} \text{symmetric parings} \\ \langle\ ,\ \rangle_V : V \otimes_{\mathbb{Z}_p} V \to 1 + m_R \\ \langle\ ,\ \rangle_W : W \otimes_{\mathbb{Z}_p} W \to 1 + m_R \\ \text{such that} \\ \langle u, T(w) \rangle_V = \langle F(v), w \rangle_W,\ \forall v \in V, w \in W \end{array} \right\}$$

where R runs through artinian local rings with residue field $\Bbbk$.
When $v_1, \cdots, v_g$ and $w_1, \cdots, w_g$ are respectively $\mathbb{Z}_p$-basis of V and W the previous result can be interpreted to the following linear algebra relations.

$$\{F(v_i) = w_i \text{ and } F(v_{a+i}) = p \cdot w_{a+i}\} \text{ and } \{T(w_i) = p \cdot v_i \text{ and } T(w_{a+i}) = v_{a+i}\} \text{ for } 1 \leqslant i \leqslant a$$

where $p^a = |V/T(W)|$ and using the symmetric pairing condition one obtains the following relation:

$$\left\{ \begin{array}{ll} \langle v_i, pv_j \rangle_V = \langle w_i, w_j \rangle_W & \text{for } 1 \leqslant i, j \leqslant a \\ \langle v_\mu, pv_i \rangle_V = \langle pw_\mu, w_i \rangle_W & \text{for } 1 \leqslant i \leqslant a,\ a+1 \leqslant \mu \leqslant g \\ \langle v_i, v_\mu \rangle_V = \langle w_i, w_\mu \rangle_W, & \text{for } 1 \leqslant i \leqslant a,\ a+1 \leqslant \mu \leqslant g \\ \langle v_\mu, v_\nu \rangle_V = \langle w_\mu, w_\nu \rangle_W, & \text{for } a+1 \leqslant \mu, \nu \leqslant g \end{array} \right.$$

Summary, for every artinian local module, the functor in [CN90, Theorem Pages:12-13] defines a symmetric pairing such that at a geometric point $(\phi : A_{/\Bbbk} \longrightarrow B_{/\Bbbk}, \lambda_A, \lambda_B)$ of the locus $\mathfrak{A}^0_{g,\Gamma_0(p)}$ of the Siegel moduli espace $\mathfrak{A}_{g,\Gamma_0(p)}$, the polynomial system $\mathfrak{S} = 0$ given by the following g^2 functions:

$$\mathfrak{S} = \left\{ \begin{array}{ll} \langle v_i, pv_j \rangle_V - \langle w_i, w_j \rangle_W & \text{for } 1 \leqslant i, j \leqslant a \\ \langle v_j, pv_i \rangle_V - \langle pw_j, w_i \rangle_W & \text{for } 1 \leqslant i \leqslant a,\ a+1 \leqslant j \leqslant g \\ \langle v_i, v_j \rangle_V - \langle w_i, w_j \rangle_W, & \text{for } 1 \leqslant i \leqslant a,\ a+1 \leqslant j \leqslant g \\ \langle v_i, v_j \rangle_V - \langle w_i, w_j \rangle_W, & \text{for } a+1 \leqslant i, j \leqslant g \end{array} \right.$$

satisfies the condition:

$$\mathfrak{S}(\hat{\phi}, \phi) = 0.$$

By using the symmetric properties of bilinear form $\langle\ ,\ \rangle_V$ and $\langle\ ,\ \rangle_W$, we see that the system $\mathfrak{S} = 0$ can be defined knowing only the following the values:

$$\begin{array}{ll} \langle v_i, v_j \rangle_V \quad \text{for } 1 \leqslant i \leqslant j \leqslant a, & \langle w_\nu, w_\mu \rangle_W, \quad \text{for } 1 \leqslant \nu \leqslant \mu \leqslant g \\ \langle v_i, v_\mu \rangle_V \,(= \langle w_i, w_\mu \rangle_W)\,, & \text{for } 1 \leqslant i \leqslant a,\ a+1 \leqslant \mu \leqslant g \end{array}$$

Indeed, the scheme $\mathfrak{A}^0_{g,\Gamma_0(p)}$ of ordinary points of $\mathfrak{A}_{g,\Gamma_0(p)}$ is smooth of dimension $g\dfrac{(g+1)}{2}$ over $\mathrm{Spec}(\mathbb{Z}_p)$ [CN90, Theorem 3.3, Page: 13].

Therefor, we consider the vector function $\mathfrak{S}$ defined by only these $g\dfrac{(g+1)}{2}$ functions.

Proposition A.1. *(Conditions de Kronecker)*
For every geometric point $(\Sigma : A_{/\Bbbk} \longrightarrow A^{\Sigma}_{/\Bbbk}, \lambda_A)$ *of the ordinary locus* $\mathfrak{A}^0_{g,\Gamma_0(p)}$*, the Jacobian matrices of the system* $\mathfrak{S} = 0$ *satisfies the following conditions:*

- $\dfrac{\partial \mathfrak{S}}{\partial X}(\hat{\Sigma}, \Sigma)$ *annihilates modulo p,*
- $\dfrac{\partial \mathfrak{S}}{\partial Y}(\hat{\Sigma}, \Sigma)$ *is invertible modulo p.*

Proof. Let us do it first for the case dimension $g = 1$, Let V and W representing respectivelly the Tate $\mathbb{Z}_p$-modules A and A^{σ} of geometric point $(\Sigma : A_{/\Bbbk} \longrightarrow A^{\Sigma}_{/\Bbbk}, \lambda_A, \lambda_{A^{\Sigma}_{/\Bbbk}})$. Then over $\mathbb{Z}_p$ we have: $V = \langle v \rangle$ and $W = \langle w \rangle$. By considering the notations above, we denote T the lineair induicing by the Verschiebung from $A^{\sigma}_{/\Bbbk}$, then $\#\left(V/T(W)\right) = p$ i.e $a = 1$. In this case, the system $\mathfrak{S} = 0$ admit a unique equation defined by the value:

$$\mathfrak{S} = \langle v, T(w) \rangle_V - \langle F(v), w \rangle_W$$

Therefor when we set: $\langle v, v \rangle = X$ and $\langle w, w \rangle = Y$ at the geometric point of $\mathfrak{A}^0_{g,\Gamma_0(p)}$, in other hand the equation is given by:

$$\mathfrak{S} = \langle v, p.v \rangle - \langle w, w \rangle = X^p - Y$$

Hence :

- $\dfrac{\partial \mathfrak{S}}{\partial X}(\hat{\Sigma}, \Sigma) = pX^{p-1}$ annihilates modulo p at any point $(\hat{\Sigma}, \Sigma)$ of $\mathfrak{A}^0_{g,\Gamma_0(p)}$;
- $\dfrac{\partial \mathfrak{S}}{\partial Y}(\hat{\Sigma}, \Sigma) = -1$ is invertible modulo p, indeed the geometric point $(\hat{\Sigma}, \Sigma)$ is on the 1-dimensional ordinary locus $\mathfrak{A}^0_{g,\Gamma_0(p)}$ over $\mathbb{Z}_p$.

In general, when the dimension is g we have $\#\left(V/T(W)\right) = p^g$ i.e $a = g$. Then the elementary functions defining the vector function $\mathfrak{S}$ are in the form:

$$X^p_{ij} - Y_{ij} \quad \text{pour} \quad 1 \leqslant i \leqslant j \leqslant g$$

Then, set $X_{ij} = \langle v_i, v_j \rangle$ and $Y_{ij} = \langle w_i, w_j \rangle$ for $1 \leqslant i \leqslant j \leqslant g$ we get:

- $\dfrac{\partial \mathfrak{S}}{\partial X}(\hat{\Sigma}, \Sigma)$ annihilates modulo p;
- $\dfrac{\partial \mathfrak{S}}{\partial Y}(\hat{\Sigma}, \Sigma) = -\,\mathrm{Id}_m$ is invertible modulo p, indeed the geometric point $(\hat{\Sigma}, \Sigma)$ is on the $m = g\dfrac{(g+1)}{2}$-dimensional ordinary locus $\mathfrak{A}^0_{g,\Gamma_0(p)}$ over $\mathbb{Z}_p$.

□

Remark A.2. Let us recall some different facts between the canonical stack structure of the $\mathfrak{A}_{g,\Gamma_0(p)}$ and the coarse structure of the scheme $\widehat{\mathfrak{A}}_g$. In the sections above, we worked on the subscheme of the ordinary locus of the coarse moduli space $\widehat{\mathfrak{A}}_g$ parameterized by modular Siegel or Hilbert polynomials rather than on the fine moduli space $\mathfrak{A}_{g,\Gamma_0(p)}$. A considerable difference between the canonical "stack" structure of $\mathfrak{A}_{g,\Gamma_0(p)}$ and the "coarse" structure of $\widehat{\mathfrak{A}}_g$ is that some

points of $\mathfrak{A}^0_{g,\Gamma_0(p)}$ are not smooth on the scheme $\widehat{\mathfrak{A}}_g$. Indeed these points represent abelian varieties having additional automorphisms. For example, In dimension 2 the points on $\mathcal{M}_2$ with $\mathrm{Aut}(\mathcal{C}) \not\simeq C_2$ or the points $j = 0,\ 1728$ on the modular curve in dimension 1. The locus of smooth points of $\mathfrak{A}_g$ is birationally equivalent to the scheme described by the modular equation. When $g = 1$, using "blowups" operations one can make this modular scheme smooth at the ordinary points (with trivial automorphisms) of $\mathfrak{A}_g$, to make it a coarse moduli space. This could well extend the domain of the Kronecker conditions in dimension 1 to points $j \in \mathbb{F}_{p^2}$ of $\mathfrak{A}_{1,\Gamma_0(p)}$ except for $j = 0,\ 1728$ (in dimension 1, the Kronecker condition domain was $j \notin \mathbb{F}_{p^2}$).However, according to [Qin93] blowups are only sufficient to smooth over a curve, ie $g = 1$.

A.3. **Lifting a Roots of Polynomial.** We recall that for an ordinary elliptic curve E over $\mathbb{F}_q$ the kernel of the Verschiebung σ is defined by a monic separable factor h of the p-division Ψ_p given by :

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

Let H be the lift of h over $\mathbb{Z}_q$, then $H(x) = h(x) \mod p$ is square free and $\Psi_p(x) \equiv H(x)^p \mod p$ i.e modulo p, the factors $H(x)$ and $\Psi_p(x)/H(x)$ are not coprime. And when $\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$ satisfies $\tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{ur}) \neq \{\mathcal{O}\}$, from [Sat00, Lemma 3.7.]:

$$\mathrm{ord}_p\left(\Psi'_p(x_P)\right) = 1 \quad \text{where} \quad \Psi'_p = \frac{\partial \Psi_p}{\partial x} \quad \text{for any} \quad P \in \tilde{E}(\mathbb{Z}_q^{ur}) - \{\mathcal{O}\}$$

Fortunately if $p \geqslant 3$, then $ker(\hat{\Sigma}) = \tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{ur})$ where $\mathbb{Z}_q^{ur}$ is the valuation ring of the maximal unramified extension ${\mathbb{Q}_q}^{ur}$ of $\mathbb{Q}_q$ [Sat00, Lemma]. However these conditions are not convenient for a standard Hensel algorithm. Since $\Psi_p(x) \equiv H(x)^p \mod p$, we have $\mathrm{ord}_p \Psi_p(x_P) \geqslant 2$ for every $P \in E[p]$ then following method compute efficiently $x_{\tilde{P}}$.
We set $f^{<n>} = n!.f^{(n)}$ for any $f = \sum a_i.X^i \in \mathbb{Z}_q[a_i, X]$.

Lemma A.3. *Let p be a prime, let f be a polynomial over $\in \mathbb{Z}_q$ and $x \in \mathbb{Z}_q$ such that $ord_p f(x) = k$ and $\mathrm{ord}_p f'(x) = e$ with $e < k$. Then for any solution r of the equation*

$$f(x) + f^{<1>}(x)p^{(k-e)}r + \cdots + f^{<i-1>}(x)p^{(i-1)(k-e)}r^{i-1} \equiv 0 \mod p^{i(k-e)} \tag{2}$$
$$\text{where} \quad i = \lceil (k+1)/(k-e) \rceil$$

$x + p^{(k-e)}r$ is a solution of f at the precision $p^{i(k-e)}$.

In the case where $k > 2e$ i.e $2(k-e) > k$, the Equation (2) gives an unique solution modulo $p^{2(k-e)}$ which converges to a unique lift without lost of precisions on x. Hence for a solution modulo p, the condition $\mathrm{ord}_p f(x) > 2\,\mathrm{ord}_p f'(x)$ ensures together the existence and unicity of the lift over $\mathbb{Z}_q$. Indeed

$$f'(x + p^{(k-e)}r) = f'(x) + f"(x)p^{(k-e)}r + \cdots + f^{<i>}(x)p^{i(k-e)}r^i + p^{(i+1)(k-e)}(\cdots)$$

implies that $\mathrm{ord}_p f'(x + p^{(k-e)}r) = e$.

Proof. Suppose that $\mathrm{ord}_p f(x) = k$ and $\mathrm{ord}_p f'(x) = e$ with $e < k$. The Taylor expansion of f is :

$$f(x + \Delta) = f(x) + f'(x).\Delta + f"(x) \cdot \Delta^2 + \cdots + f^{<i-1>}(x)\Delta^{i-1} + \Delta^i \cdot Q(x)$$

where $Q(x)$ is in $\mathbb{Z}_q$.
Set $\mathrm{ord}_p(\Delta) = m$ we want to determine the error r at precision p at less, necessarily $f(x)$ and $f'(x).\Delta$ must be at the same precision then $m = k - e$. Therefor we can solve the equation (in function of r) at precision $p^{i(k-e)}$ such that $i(k-e) = k+1$ i.e $i = \lceil (k+1)/(k-e) \rceil$.

$$f(x) + f^{<1>}(x)p^{(k-e)}r + \cdots + f^{<i-1>}(x)p^{(i-1)(k-e)}r^{i-1} \equiv 0 \mod p^{i(k-e)}$$

□

When $k \leqslant 2e$ the resolution of the Equation (2) depends on the valuations of the $f^{<j>}(x)$'s for $2 \leqslant j \leqslant i(k-e)$. The Equation (2) may have solution on an extension or no solutions any where. For instance:
• If there exists only one $j \in \{2,\ i(k-e)\}$ such that $\mathrm{ord}_p\, p^{j(k-e)} f^{<j>}(x)$ is lesser than k then r does not exists.
• If $\mathrm{ord}_p\, p^{j(k-e)} f^{<j>}(x)$ is greater or equal to $i(k-e)$ for all $j \in \{2, i(k-e)\}$, then in this case each solution of Equation (2) defines a lift of x over $\mathbb{Z}_q$.

Example A.4. Let p be an odd prime and E an elliptic curves over $\mathbb{F}_q$, we recall that for $P(x_0, y_0) \in E[p]$, $\mathrm{ord}_p\, \Psi_p(x_0) > 1$, $\mathrm{ord}_p\, \Psi'_p(x_0) = 1$, and furthermore since $\Psi_p = h^p \mod p$, we have $\mathrm{ord}_p\, \Psi"_p(x_0) \geqslant 1$. Then we have $\mathrm{ord}_p\, \Psi_p(x_0) \geqslant 2.\, \mathrm{ord}_p(\Psi'_p(x))$ and the previous Lemma A.3 allows to compute the unique lift of x_0 over $\mathbb{Z}_q$.
For instance when $\mathrm{ord}_p\, \Psi_p(x_0) = 2$, we have $k = 2$ and $e = 1$ then the equation in lemma A.3 becomes :

$$\Psi_p(x_0) + \Psi'_p(x_0).p.r \equiv 0 \mod p^3 \quad \text{since} \quad \mathrm{ord}_p\, \Psi"_p(x_0) \geqslant 1.$$

For $k \geqslant 3$, $2(k-e) > k$ one can solve the equation Lemma A.3 modulo $p^{2(k-e)}$.

$$\Psi_p(x) + \Psi'_p(x).p^{(k-e)}.r \equiv 0 \mod p^{2(k-e)}.$$

We recall that T.Satoh has introduced in [Sat00, Lemma 2.1] a variant of Hensel's lift that compute the lift of the representative polynomial h of $E[p]$ over $\mathbb{Z}_q$. In small characteristics $\#E[p]$ is small and the previous method of Lemma A.3 becomes faster since Satoh use in each step the extended gcd algorithm to compute the error r.

Whenever $\mathrm{ord}_p\, f(x) \leqslant e$ one can apply the following method to obtain a sufficient precision corresponding to the Lemma A.3. The strategy is simple but it not ensures any convergence for a solution, the goal is to reach the previous condition of convergence (described in Lemma A.3). To determine the error r we need a $f^{<j>}(x)$ and $\alpha \in \mathbb{N}$ such that $\mathrm{ord}_p(f^{<j>}(x)p^{j\alpha}) = \mathrm{ord}_p\, f(x)$. We suppose that a root $\tilde{x} \in \mathbb{Z}_q$ of f exists and we know that $x = \tilde{x} \mod p$.

Lemma A.5. *Let* $\mathrm{ord}_p\, f(x) = k$ *and* $\mathrm{ord}_p\, f'(x) = e$ *such that* $1 < k \leqslant e$. *Let* j *be the smallest positive integer (if it exists) such that* $\mathrm{ord}_p(f^{<j>}(x)) + j \leqslant k$. *Then for any solution* r *of the equation*

$$f(x) + f^{<1>}(x).p^{\alpha}.r + \cdots + f^{<j>}(x).p^{j\alpha} r^j \equiv 0 \mod p^{(j+1)\alpha} \tag{3}$$

$$\textit{where} \quad \alpha = \lfloor \frac{k - \mathrm{ord}_p(f^{<j>}(x))}{j} \rfloor;$$

$x + p^{\alpha} r$ *is solution of* f *at the precision* $p^{(j+1)\alpha}$.
Further if $\mathrm{ord}_p(f^{<j>}(x)) \leqslant \alpha$ *then* $\mathrm{ord}_p\, f'(x + p^{\alpha} r) < (j+1)\alpha$ *(hypothesis of Lemma A.3).*

Obviously one can remark that such j is less or equal to $(\deg f + 1)$.
The situation $\mathrm{ord}_p(f^{<j>}(x)p^{j\alpha}) < k$ in this Lemma A.5 happens mostly when at this stage x is not at good precision. And at this precision f has many roots but not all lift to the unknown $\tilde{x}$.

Proof. For simplicity we suppose $\mathrm{ord}_p\, f^{<j>}(x) = 0$.
In the Taylor expansion Equation (3), we have enough precision to divide by $\mathrm{ord}_p(f^{<j>}(x)p^{j\alpha})$ and we get modulo p^{α}) an equation:

$$a_j r^j + \cdots a_1 r + a_0 = 0 \quad \text{with} \quad a_i \in \mathbb{Z}_q.$$

The possible vanishing factor modulo p^{α} contains the errors for the next precision. For a root r of the previous equation we have: $f(x + p^{\alpha} r) = 0 \mod p^{(j+1)\alpha}$. Further if $\mathrm{ord}_p\, r = 0$, then the

relation

$$f'(x+p^\alpha r) = f'(x) + f^{<2>}(x).p^\alpha r + \cdots + f^{<j>}(x).p^{j\alpha}r^j + p^{(j+1)\alpha}(\cdots)$$

implies that $\text{ord}_p\, f'(x+p^\alpha r) = j\alpha < (j+1)\alpha$ since only $\text{ord}_p(p^{j\alpha}f^{<j>}(x)) \leqslant k$. □

Remark A.6.

Interpretation. We want to explain on other hand the link between the previous methods and the standard Hensel's algorithm (based on the fact $\text{ord}_p\, f'(x) = 0$). In the both situations (Lemmas A.3 and A.5) the error computation run like in the standard Hensel method by modifying the function f in a neighborhood of the approximation x. Therefor in the case when the lift $\tilde{x}$ exists we are able to extract an approximation of the function f which satisfies the standard Hensel condition. For instance:

- In the case where $\text{ord}_p\, f(x) > 2{\cdot}\text{ord}_p\, f'(x)$ the local function is defined in a neighborhood of x (the ball of center x and radius p^{k-e}) by $g = p^{-e}f$ hence we have $\text{ord}_p\, g(x) = k-e$ and $\text{ord}_p\, g'(x) = 0$.
- The case of Lemma A.5 is more complicate since it is possible to have more than one solution for the "error-equation" (Equation (3)) and each solution corresponds to an approximation of the function f in a ball of center x and radius p^α. The first goal is to reach the condition for applying Lemma A.3. For simplicity we suppose $\text{ord}_p\, f^{<j>}(x) = 0$ and the corresponding error can be computed using the approximation functions of f defined by:

  $$g = p^{-j\alpha}\left(b_0 f + b_1 f^{<1>} + \cdots + b_{j-1}f^{<j-1>}\right) \quad \text{with} \quad \text{ord}_p\, b_{j-1} = 0.$$

  Then the extracted functions satisfy $\text{ord}_p\, g'(x) = 0$ (by using the definition of j and the fact $\text{ord}_p\, f^{<j>}(x) = 0$). Specially the evaluations at x of these approximation functions are given by a factorization (in function of r) of the relation " **??** " in prime factors over $\mathbb{Z}_q$ at precision p^α (the Newton condition). Therefor in each "Taylor branch" (defined by an associated r) the next steps converge to a unique lift over $\mathbb{Z}_q$.

Number of lifted roots. Let $f \in \mathbb{Z}_q[X]$ and $\tilde{x}$ be a root of f over $\in \mathbb{Z}_q$ such that $ord_p f(x) = k$ and $ord_p f'(x) = e$.

- If $k > 2e$ then only one root of f over $\mathbb{Z}_q$ reduces to x modulo p^k.
- Otherwise the number of roots of f over $\mathbb{Z}_q$ that reduce modulo p^k to x can be more.

The methods detailed previously allow under certain conditions to lift a root of a polynomial in $\mathbb{Z}_q[X]$ without loss of precision in the best cases. Hence it computes a p-torsion point of a canonical lift of an ordinary elliptic curves.
Next we want to generalize these methods to the case of multivariate polynomials system of dimension zero in the sense to compute the lift of the p-torsion on an abelian varieties.

A.4. **Lifting a Solution in Polynomial System.** Let F be the vector function of a multivariate polynomial system $F = 0$ over $\mathbb{Z}_q$ of dimension zero and let DF be its Jacobian matrix. We suppose that $\tilde{X}$ a root of F over $\mathbb{Z}_q$ exists and we know its approximation X (at unknown precision) such that $\text{ord}_p\, F(X) = k$, $\text{ord}_p \det(DF(X)) = e$ and $\tilde{X} = X \mod p$. Generally the components of X can be at different precisions (comparing to the components of $\tilde{X}$). Therefor we need first to exhibit the precision of each component of X. And by separating the errors in the components we know the method corresponding to each "error-equation".
Let S be the Smith Normal Form of the Jacobian matrix $DF(X)$ of F at X such that $DF(X) = M \cdot S \cdot N$ with M and N invertible. Then we get $DG(X) = M^{-1} \cdot DF(X) \cdot N^{-1} = S$ and $G(X) = M^{-1} \cdot F(XN^{-1})$ with $DG(X) = \text{diag}(p^{e_1}, p^{e_2}, ..., p^{e_n})$ and $e = e_1 + \cdots + e_n$.

Proposition A.7. *Suppose that each component X_i of X is at precision p^{k_i}. Then one can find in quadratic time the approximations of $\tilde{X}$ at precision $N > k_i$ by using:*

- *the method of Lemma A.3 if each $k_i > e_i$;*
- *otherwise the one of Lemma A.5*

Proof. The information on the valuations given by the calculation of SNF is necessary in the absence of a known result on the Jacobian matrix (like in Section 4 and Proposition 4.1).
The base change does not affect the errors that we want to determine; we start from the system with G given by the Smith Normal Form on F, then the Newton algorithm in X will work similarly to the univariate case (of the above lemmas) When we have $\mathrm{ord}_p G_i(X_i) = k_i$ with $k_i > e_i$ for all i then the lifts of X (at precision $N > \max(k_i)$) can be computed using the method Lemma A.3. Otherwise, some equations need additional information, so globally we compute the other successive derivatives as suggested in the method Lemma A.5. Thus, we determine the approximations of the lifts (corresponding to Lemma A.3 at the next step) .
From the Taylor expansion of F at $(X + Rp^k)$, a lexicographic Groebner basis computation in function of the components of the error R at precision p^N allows compute the error R for next stage. □

Cheikh Anta Diop University, Dakar, SENEGAL

Équipe FAST, LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées)
Email address: abdoulaye.maiga@ucad.edu.sn

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)