FAST ADDITION ON NON-HYPERELLIPTIC GENUS 3 CURVES

STÉPHANE FLON, ROGER OYONO, AND CHRISTOPHE RITZENTHALER

ABSTRACT. We present a fast addition algorithm in the Jacobian of a genus 3 non-hyperelliptic curve over a field k of any characteristic. When the curve has a rational flex and k is a finite field of characteristic greater than 5, the computational cost for addition is $163M + 2I$ and $185M + 2I$ for doubling. We study also the rationality of intersection points of a line with a quartic and give geometric characterizations of $C_{3,4}$ curves and Picard curves. To conclude, an appendix gives a formula to compute flexes in all characteristics.

INTRODUCTION

In this article, we present a simple geometric algorithm for addition in the Jacobian of non-hyperelliptic genus 3 curves, represented as smooth plane quartics. Several articles have been written on the subject (see Section 5 for a discussion) and the present one continues this work by providing a straightforward generalization of [8, 3, 23]. Our contribution is at three different levels:

(1) we have devoted special care in writing the algorithm to minimize the number of operations. Thus, our algorithm is to date the fastest one for arithmetic in the Jacobian of a 'general' (see below) non-hyperelliptic genus 3 curve over a finite field k of characteristic greater than 5. As in previous articles, we measure the complexity by counting the number of multiplications M and inversions I that need to be performed in k. The computational cost for addition is $163M + 2I$ and $185M + 2I$ for doubling. Note that [22] has announced $117M + 2I$ for addition and $129M + 2I$ for doubling for $C_{3,4}$ curves which makes it the fastest algorithm for this special case.

(2) we present several mathematical results on the arithmetic of plane quartics. Indeed, the efficiency of our algorithm depends on the existence of a rational line l^∞ cutting the quartic in rational points only. We announce in this article that if $\#k \geq 127$ there always exists such a line (Theorem 1) and if $\#k \geq 66^2 + 1$ and $\text{char}(k) \neq 2$ then l^∞ can be chosen tangent to the quartic C (Theorem 2). We then study the remaining cases: we show heuristically that any quartic has a line

l^∞ such that $(l^\infty \cdot C) = 3P + Q$ with $P, Q \in C(k)$ with probability about 0.63 (P is called a flex point). We call this case the 'general case'. We finally show that quartics with a rational hyperflex (i.e. $P = Q$ with the previous notations) represent exactly the case of $C_{3,4}$ curves (Proposition 2) and we characterize among them Picard curves as the curves with a rational Galois point (Proposition 3).

(3) To confirm our heuristic probability, we made tests which required the computation of flexes. As far as we know, the most general method was due to Abhyankar [1] which works for all but characteristic 2. In this article, we present the first formula to compute the flexes in all characteristics.

Due to recent progress in index calculus attacks (see [6]), it appears unlikely that genus 3 non-hyperelliptic curves may be used for building discrete logarithm cryptosystems. However, as in [22], we point out that the results presented in this paper still may be useful for cover attacks on discrete logarithms of other curves particularly in connection with Weil descent. Moreover, as illustrated in Section 4, fast addition algorithms can be useful in some recent point counting algorithm, like the AGM or those based on modular curves.

The article is organized as follows. In the first section we present the geometric description of our algorithm. Section 2 deals with the rationality issues of the intersection of a line and a plane quartic over a finite field. Section 3 deals with the translation of the geometry in an algebraic language, thanks to Mumford representation. We write down the operations performed in the tangent case and we optimize our algorithm in the flex case. Section 4 shows examples of application of our algorithm. The conclusion summarizes and compares complexities of already existing methods. Finally an appendix proves our formula to compute the flexes and gathers tables which describe in details the operations for addition and doubling in the 'general' case.

1. Geometric description of the algorithm

Let C be a non-singular curve of genus g over a field k. Let D^∞ be an effective k-rational divisor of degree g. A consequence of Riemann-Roch theorem is the following representation of divisors:

Fact (Representation of divisors). *Let D be a rational degree 0 divisor of C. Then there exists a rational effective divisor D^+ of degree g such that $D^+ - D^\infty \sim D$. Generically, the divisor D^+ is unique.*

We now restrict ourselves to the case where C is a genus 3 non-hyperelliptic curve. Thanks to the canonical embedding, we may assume that C is a smooth plane quartic. Conversely, any smooth plane quartic is a genus 3 non hyperellipic curve. We denote by x, y, z (or sometimes x_1, x_2, x_3) coordinates in $\mathbb{P}^2$.

We denote by $(*)$ the following condition: *There is a rational line l^∞ which crosses C in four (not necessarily distinct, but with multiplicity then) k-points $P_1^\infty, P_2^\infty, P_3^\infty, P_4^\infty$.*

Until the end of this section, we assume that condition $(*)$ is fulfilled (see Section 2 for a discussion on this topic when k a finite field).

We choose D^∞ to be the divisor $P_1^\infty + P_2^\infty + P_3^\infty$.

By abuse of language we say that a curve C' *goes through* nP if $i(C, C'; P) = n$, where $i(C, C'; P)$ denotes the intersection multiplicity of C and C' at P.

Proposition 1. *Let $D_1, D_2 \in Jac(C)(k)$. Then $D_1 + D_2$ is equivalent to a divisor $D = D^+ - D^\infty$, where the points in the support of D^+ are given by the following algorithm:*

(1) *Take a cubic E defined over k which goes (with multiplicity) through the support of D_1^+, D_2^+ and $P_1^\infty, P_2^\infty, P_4^\infty$. This cubic also crosses C in the residual effective divisor D_3.*

(2) *Take a conic Q defined over k which goes through the support of D_3 and P_1^∞, P_2^∞. This conic also crosses C in the residual effective divisor D^+.*
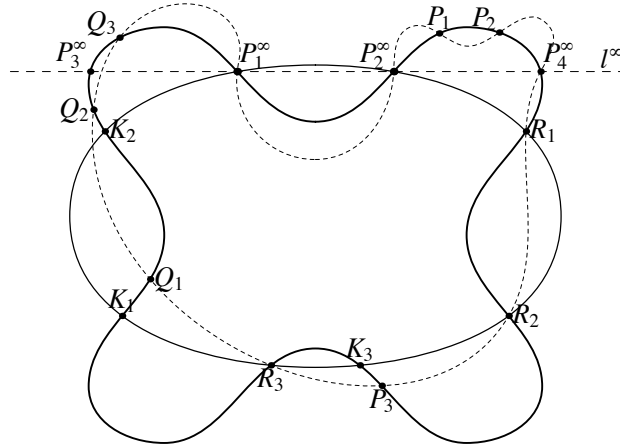

FIGURE 1. Description of the algorithm

Proof. C being canonically embedded, $(E \cdot C) \sim 3\kappa$ where $\kappa = \kappa_C$ is the canonical divisor of C. Therefore we have

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + D_3 \sim 3\kappa.$$

Similarly, $(Q \cdot C) \sim 2\kappa$ so

$$D_3 + P_1^\infty + P_2^\infty + D_e \sim 2\kappa$$

and $(l^\infty \cdot C) = P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty \sim \kappa$. Combining these three relations, we obtain

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + D_3 \sim D_3 + P_1^\infty + P_2^\infty + D_e + P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty$$

so

$$D_1^+ + D_2^+ \sim D_e + D^\infty.$$

Now we subtract $2D^\infty$ on both sides:

$$D_1 + D_2 \sim D_e - D^\infty \sim D$$

So $D_e = D^+$.

The cubic E and conic Q are both defined over the field k because of the k-rationality of P_i^∞, D_1^+ and D_2^+. $\square$

Remark. Actually, we need a milder hypothesis than $(*)$: it would be enough to have a line l^∞ such that P_3^∞, P_4^∞ are rational (this is always true over a finite field $k = \mathbb{F}_q$ with $q > 26$ see [7]). However, we need $(*)$ in order to simplify the equations of the different curves involved and optimize the algorithm (see Section 3).

2. RATIONALITY OF THE POINT ON A CANONICAL DIVISOR

2.1. **Structure of the canonical divisor.** Let C be a smooth plane quartic defined over an algebraically closed field $\bar{k}$. There are 5 possibilities for the intersection divisor $(l \cdot C) = P_1 + P_2 + P_3 + P_4$ of a line l with C:

   (1) The four points are pairwise distinct. This is the generic position.
   (2) $P_1 = P_2$, then l is tangent to C at P_1.
   (3) $P_1 = P_2 = P_3$. The point P_1 is then called a *flex*. As a linear intersection also represents the canonical divisor, these points are exactly the ones where a regular differential has a zero of order 3. They are thus the Weierstrass points of C. The quartic C has infinitely many flexes if and only if $\mathrm{char}(\bar{k}) = 3$ and C is isomorphic to the Fermat quartic $x^4 + y^4 + z^4 = 0$ (see [25, p.28]).
   (4) $P_1 = P_2$ and $P_3 = P_4$. The line l is called a *bitangent* of the curve C and the points P_i *bitangence points*. It is well known (see for example [19]) that if $\mathrm{char}(\bar{k}) \neq 2$ then C has exactly 28 bitangents. If $\mathrm{char}(\bar{k}) = 2$, then C has respectively $7, 4, 2,$ or 1 bitangents, according to the 2-rank of its Jacobian (resp. $3, 2, 1, 0$).
   (5) $P_1 = P_2 = P_3 = P_4$. The point P_1 is called a *hyperflex*. Generically, such a hyperflex does not exist (*i.e.* the set of quartics with at least one hyperflex is of codimension 1 in the space of quartics). The number of hyperflexes is less than 12 if C is not isomorphic to the Fermat quartic over a field of characteristic 3. Moreover in this later case, the number of hyperflexes of C is equal to 28 (all the bitangence points are hyperflexes) (see [25, p.30]).

The efficiency of the algebraic version of the algorithm will depend on the choice of l^∞ (see Section 3). Roughly speaking, 'the more special the faster'. However, it is not clear for which choice of l^∞, the condition $(*)$ is fulfilled. We now study this condition when k is a finite field. For the general and tangent cases, we only state results whose proofs will be given in a forthcoming article [9].

In this section, we assume that k is a finite field $\mathbb{F}_q$ (with $q = p^n$ for a certain prime p).

2.2. **The general and tangent case.** Using the same techniques as in [6], we can prove the following result.

Theorem 1 ([9]). *Let C be a smooth plane quartic over $\mathbb{F}_q$. If $q \geq 127$, there exists a line which cuts C at rational points only, i.e. C satisfies the condition $(*)$.*

For the tangent case, we had to build a more elaborate strategy based on correspondence curves.

Theorem 2 ([9]). *Let C be a smooth plane quartic over $\mathbb{F}_q$ and assume that $char(k) \neq 2$. If $q \geq 66^2 + 1$, there exists a tangent at C which cuts C at rational points only, i.e. C satisfies $(*)$ for a tangent line.*

Remark. We have been so far unable to extend the proof to the characteristic 2 case. We hope to solve this problem in a near future.

2.3. **The flex case.** Let us assume that C has a rational flex. Then the tangent at this point is a line satisfying $(*)$. Unfortunately, we do not know how to compute the probability for a quartic to have at least a rational flex. But we can have a guess on that number, coming from heuristic remarks on one side, and relying on numerical evidences on the other side.

Conjectural fact. *The probability that a smooth plane quartic has at least one rational flex is asymptotically, when q tends to ∞, equal to $1 - e^{-1} + \alpha > 0.63$, with $|\alpha| \leq 10^{-25}$.*

Proof. (heuristic) Here we suppose that $char(k) > 3$. Let $C : f = 0$ be the curve and $H(f) : h = 0$ its Hessian (see Appendix). The curve $H(f)$ is of degree 6 and the $(C \cdot H(f))$ are the 24 flexes with multiplicities. Generically, when $q >> 0$ we may suppose that no two flexes have the same abscissae. Then there is a rational flex if and only if the polynomial $\mathrm{Res}(f, h, y)$ has a root in k. If we suppose that these polynomials are uniformly distributed among the polynomials of degree 24, then one only has to compute the probability that a polynomial of degree 24 has at least one linear factor in $\mathbb{F}_q$. Let $(\alpha_i)_{i \in \{1,\ldots,q\}}$ be an enumeration of $\mathbb{F}_q$.

Let S be the set of all monic polynomials of degree n and S_i the subset of S of polynomials having one or more factors of the form $x - \alpha_i, i = 1, \ldots, q$. Then $\#S = q^n$ and $\#S_i = q^{n-1}$. By inclusion-exclusion principle, the number $N(n, q)$ of monic polynomials of degree n with one or more linear factors is equal to

$$N(n, q) = \sum_{i=1}^{n} \binom{q}{i} q^{n-i} (-1)^{i-1} \quad \text{if } n < q,$$

and

$$N(n, q) = \sum_{i=1}^{q} \binom{q}{i} q^{n-i} (-1)^{i-1} \quad \text{if } n \geq q.$$

After straightforward computations, one computes that the probability $P(n, q)$ that a monic polynomial of degree n has at least a linear factor in $\mathbb{F}_q$ is

$$P(n, q) = 1 - \left(1 - \frac{1}{q}\right)^q - \beta_n(q),$$

where

$$|\beta_n(q)| \leq \frac{1}{(n+1)!} \quad \text{and hence} \quad \lim_{\substack{n < q \\ n, q \to \infty}} \beta_n(q) = 0.$$

Already for $n = 24$ and $q = 25$ we have $|\beta_n(q)| = 25^{-25} \leq 1.13 \cdot 10^{-35}$. $\quad \square$

We made numerical experiments to support our heuristic argument as well as to check the conjecture in characteristics 2 and 3. In these two cases,

we have indeed $H(f) \equiv 0$. However, we have been able to find a good substitute for $H(\mathrm{f})$, see Section 6.

Computations realized with a bench of 10^6 non-singular quartics give the right percentage. Thus the conjecture seems to hold.

p	n	Probabilities
2	17	$632074/10^6 = 0.632074$
3	11	$632344/10^6 = 0.632344$
1009	2	$631358/10^6 = 0.631358$
$2^{17} + 29$	1	$632921/10^6 = 0.632921$

2.4. **The hyperflex case.** We recall that a generic non-singular quartic has no hyperflex. If C has a rational hyperflex, then we find special curves already treated in the literature, namely $C_{3,4}$ curves. Recall that a C_{ab} curve is a nonsingular curve X/k for which there exists a cover $\varphi : X \to \mathbb{P}^1$ in which a k-rational point P is totally ramified. Such a curve admit a plane affine model

$$X : \alpha_{0,a}\, y^a + \alpha_{b,0}\, x^b + \sum_{ia+jb<ab} \alpha_{i,j}\, x^i y^j = 0,$$

with $\alpha_{i,j} \in k$ and $\alpha_{b,0}, \alpha_{0,a} \neq 0$.

Proposition 2. *A non-singular plane quartic C with a rational hyperflex P is k-isomorphic to a $C_{3,4}$ curve of genus 3.*

Proof. By a linear rational transformation, we may suppose that P is the point $(0 : 1 : 0)$ and that the tangent at this point is the line at infinity, i.e. the line with equation $z = 0$. Therefore the equation of C is of the form

$$y^3 + h_1 y^2 + h_2 y = f_4$$

where h_i is a degree i polynomial and f_4 is a degree 4 monic polynomial. $\qquad\square$

Remark. We can wonder whether a plane quartic with a hyperflex generically has a rational hyperflex. This is actually the case: indeed, according to [26] and if $\mathrm{char}(k) > 3$, the locus of plane quartics with more or equal than two hyperflexes has codimension one in the locus of plane quartic with a hyperflex. So plane quartics with exactly one hyperflex (thus a rational hyperflex since it has to be Galois invariant) are generic. However, one can find rational families of quartics with at least two hyperflexes which are not defined over k. For instance $x^4 + (y^2 - \alpha z^2) \cdot Q(x, y, z)$ where $Q \in k[x, y, z]$ is a homogeneous degree 2 polynomial and α is not a square in k has $(0 : \sqrt{\alpha} : 1)$ and $(0 : -\sqrt{\alpha} : 1)$ as conjugate hyperflexes.

One may like to characterize Picard curves among $C_{3,4}$ curves. Recall that if $\mathrm{char}(k) \neq 3$, a Picard curve is a genus 3 curve which admits an affine model of the form $y^3 = f_4(x)$. Clearly the four points $(\alpha_i : 0 : 1) \in C$ are flexes whose tangent goes through $P = (0 : 1 : 0)$. Conversely, it is easy to see that Picard curves are exactly the smooth plane quartics with one rational hyperflex P and 4 distinct collinear flexes $(P_i)_{i=1,\ldots,4}$ whose tangents are all concurrent at P (take $P = (0 : 1 : 0)$ and the line defined by

the P_i's as the $y = 0$ line). Another characterization, maybe more natural, is in terms of Galois point. Such points have been studied in [18] over a field of characteristic 0 and are defined as follows. Let $P \in C(\overline{k})$ and $\phi_P : C \to |\kappa_C - P| = \mathbb{P}^1$ the degree 3 morphism induced by the linear system $|\kappa_C - P|$ (i.e. the lines going through P). P is called a *Galois point* if the geometric cover defined by ϕ_P is Galois. One has the following characterization.

Proposition 3. *Let $char(k) \neq 3$. A smooth plane quartic C is a Picard curve if and only if there exists $P \in C(k)$ such that P is a Galois point.*

Proof. If C is a Picard curve, it admits a projective model $(y/z)^3 = f_4(x/z)$. Let $P = (0 : 1 : 0)$ and replace $x = tz$ for $t \in \overline{k}$. We obtain

$$\left(\frac{y}{z}\right)^3 = f_4(t).$$

This clearly defines a Galois extension of $k(\mathbb{P}^1) = k(t)$. Conversely, let assume that C is a smooth plane quartic with a Galois point $P \in C(k)$. First we show that P is a hyperflex. If the cover ϕ_P is Galois then there exists an automorphism $\alpha : C \to C$ of order 3 such that $\phi_P : C \to C/\langle\alpha\rangle$. As C is canonically embedded, α induces a projective automorphism of $\mathbb{P}^2$. We show that $\alpha(P) = P$. Let $R_1 + R_2 + R_3 = \phi_P^{-1}(t_0)$ for a generic t_0. The line $\overline{\alpha(R_1)\alpha(R_2)}$ goes through $\alpha(P)$. The morphism α permutes the R_i so $\overline{\alpha(R_1)\alpha(R_2)} = \overline{R_1 R_2}$ and $\alpha(P) = P$. The point P is then ramified in the cover ϕ_P and then is completely ramified. Thus, the tangent line to C at P cuts the divisor $4P$, i.e. P is a hyperflex.
Now if a point $Q \neq P$ is ramified then Q is completely ramified and it is then a flex. As $char(k) \neq 3$, Hurwitz formula shows that there must be exactly 4 such flexes associated to P. We can assume that $P = (0 : 1 : 0)$ with tangent $z = 0$, and that two of them are the points $P_1 = (0 : 0 : 1)$ and the point $P_2 = (1 : 0 : 1)$. As P is a hyperflex, Proposition 2 shows that C admits a model

$$y^3 + (a_1 x + a_0)y^2 + (b_2 x^2 + b_1 x + b_0)y = x(x-1)(x-r_1)(x-r_2).$$

We have the following facts:

- since the tangent at P_1 (resp. P_2) goes through P, $b_0 = 0$ (resp. $b_2 = -b_1$);
- since P_1 (resp. P_2) is a flex, the tangent at P_1 (resp. P_2) cuts the curve only at P_1 and P (resp. at P_2 and Q). So $a_0 = 0$ (resp. $a_1 = 0$).

Then we actually get a model of the form

$$y^3 + bxy(x-1) = x(x-1)(x-r_1)(x-r_2)$$

and we are done if we show that $b = 0$.
We consider separately the case $char(k) > 3$ and the case $char(k) = 2$.
If $char(k) > 3$, letting $x = tz$ we get the following equation for the cover

$$y^3 + (bt^2 - bt)y + (-t^4 + t_3(r_1 + r_2 + 1) - t^2(r_1 r_2 + r_1 + r_2) + t r_1 r_2).$$

It is classical that this extension is Galois if and only if its discriminant $\Delta \in \overline{k}(t)$ is a square (here we need that $\mathrm{char}(k) \neq 2$). Now,

$$\Delta \;=\; -27t^2 \cdot (t-1)^2 \cdot [t^4 - 2(r_1 + r_2)t^3 + (r_1^2 + r_2^2 + 4r_1r_2 + \frac{4}{27}b^3)t^2$$
$$-2(r_1 r_2^2 + r_2 r_1^2 + \frac{2}{27}b^3)t + (r_1 r_2)^2].$$

Thus Δ is a square if and only if the last factor is a square, i.e. can be written $(s_2 t^2 + s_1 t + s_0)^2$. It is easy to check that this implies $b = 0$.

If $\mathrm{char}(k) = 2$, let $P_3 = (x_3 : y_3 : z_3) \in C$ be a third flex such that its tangent goes trough P. In particular

$$\partial h / \partial y (P_3) = y_3^2 z_3 + b x_3 z_3 (x_3 - z_3) = 0.$$

We replace $y_3^2 = b x_3 (x_3 - 1)$ in the equation of C and we get

$$x_3(x_3 - 1)(x_3 - r_1)(x_3 - r_2) = 0.$$

Thus let say $x_3 = r_1$. Let $x = r_1 z$ then replacing in the equation of C, we get $zy^3 + b r_1 z^3 y (r_1 - 1) = 0$. The point $(r_1 : 0 : 1)$ is then a flex if and only if $b = 0$. □

3. ALGEBRAIC DESCRIPTION

In section 1, we gave a general geometric description of our algorithm. In this section, we will give an algebraic description in the tangent case and a completely optimized one, for implementation, in the flex case.

3.1. Mumford representation and typical divisors.
We need a simple representation for the effective divisors D^+. Let C be a smooth plane quartic satisfying $(*)$. We may suppose (after a k-linear transformation) that P_1^∞ is a point at infinity (i.e. such that its z-coordinate is 0), and that l^∞ is the line $z = 0$. Let $f(x, y) = 0$ be an affine equation of C. As in [8], we work with *Mumford representation*. A divisor $D \in \mathrm{Jac}(C)(k)$ is represented by a couple $[u, v]$ of polynomials in $k[x]$. Recall that this representation is unique under the following generic assumptions on D, which define a *typical divisor*:

(1) The three points in the support of D^+ are non-collinear. In this case D^+ is unique: in fact if $P_1 + P_2 + P_3 + (f) = Q_1 + Q_2 + Q_3$ then $f \in \mathcal{L}(P_1 + P_2 + P_3)$ and f has to be constant by the Riemann-Roch theorem.

(2) There is no point at infinity in the support of D^+. Let $P_i = (x_i : y_i : 1)$ ($i = 1, 2, 3$) be the three points in the support of D^+ and $u = \prod(x - x_i)$. Since D^+ is a rational divisor, $u \in k[x]$.

(3) The $(x_i)_{i=1,2,3}$ are distinct. In this case, there exists a unique polynomial $v \in k[x]$ of degree 2 such that $y_i = v(x_i)$ for $i = 1, 2, 3$ (it is simply the interpolation polynomial).

Conversely, given a couple $[u, v]$ such that

- $u, v \in k[x]$,
- $u = \prod(x - x_i)$ is monic of degree 3 and with simple roots,
- $\deg(v) = 2$,
- $u | f(x, v(x))$,

then $P_1 + P_2 + P_3 - D^\infty$ is a rational typical divisor of C (where, for $i \in \{1, 2, 3\}$, we have $P_i = (x_i : v(x_i) : 1)$).

Proposition 4. *Assume that k is algebraically closed, then the locus of non typical divisor is of codimension 1 in the Jacobian of C.*

Proof. Clearly if the points in the support of D^+ are collinear $l(\kappa - D^+) \neq 0$, i.e. D^+ is a special divisor. $D^+ - D^\infty$ is then contained in a translate of the theta divisor, i.e. in a variety of codimension 1.
If the second condition is not satisfied then D^+ is contained in the union $\cup_{P \in (C \cdot l^\infty)} (C + C + P)$. The image of this dimension 2 variety in the Jacobian of C is thus of codimension 1.
Let us assume (after a possible change of coordinates) that the point $(0 : 1 : 0)$ does not belong to C. Denote $\phi : C \to \mathbb{P}^1$ the projection of the x-coordinate $\phi(x : y : z) = (x : z)$. Let

$$V = \{(P_1, P_2, P_3) \in C^3, \phi(P_1) = \phi(P_2) \text{ or } \phi(P_2) = \phi(P_3) \text{ or } \phi(P_3) = \phi(P_1)\}.$$

If the third condition is not satisfied, then $D^+ - D^\infty$ belongs to the image of V in the Jacobian of C. So again, it belongs to a variety of codimension 1. □

In particular, we see that addition of two typical divisors or doubling of a typical divisor is generically a typical divisor. As we are mainly interested in implementation over large fields where we can assume that the generic hypothesis holds, we will restrict our description of the algorithms to the case of a typical divisor. Note however that the non typical cases can be handled even more efficiently than the generic case since the representation uses polynomials $[u, v]$ of lower degrees.

3.2. **The tangent case.** After a k-linear transformation, we may suppose that $l^\infty : z = 0$ is tangent at $P_1^\infty = P_2^\infty = (0 : 1 : 0)$ and goes through $P_4^\infty = (1 : 0 : 0)$. An equation for C is then of the form

$$y^3 + h_1 y^2 + h_2 y = f_3,$$

where $h_1, h_2, f_3 \in k[x]$ and $\deg(h_1) \leq 2, \deg(h_2) \leq 3, \deg(f_3) \leq 3$. We then have

Lemma 1. *The cubic E from the theorem is generically of the form*

$$y^2 + s \cdot y + t,$$

where s and t are polynomials in $k[x]$, with $\deg(s) \leq 2$ and $\deg(t) \leq 2$. The cubic Q is of the form

$$y - v,$$

where $v \in k[x]$ and $\deg(v) = 2$.

Proof. As $P_1^\infty \in E$ we see that an equation of E has no y^3 term. One can then write it in the form

$$y^2 d + sy + t$$

with d (resp. s, resp. t) polynomials in x of degree less than 1 (resp. less than 2, resp. less than 3). Now $l^\infty : z = 0$ is the tangent at E in P_1^∞ so we can assume $d = 1$. Finally $P_4^\infty \in E$ implies that E has no x^3 term. This gives the form of the cubic.

As for the cubic, the conic Q must have a tangent line at P_1^∞ equal to l^∞. This gives directly the desired form. $\qquad\square$

To explicit the coefficients of E and Q, one proceeds similarly as in [8, 2.1.2]. Note that all the computations are carried over k.

Algorithm 1 Algorithm for Addition.

INPUT: $D_1 = [u_1, v_1]$ and $D_2 = [u_2, v_2]$
OUTPUT: $D_1 + D_2 = [u_{D_1+D_2}, v_{D_1+D_2}]$

---

1. *Computation of the cubic E*

    Addition

    compute the inverse t_1 of $v_1 - v_2$ modulo u_2

    compute the remainder r of $(u_1 - u_2)t_1$ by u_2

    solve the linear equations given by the following conditions

    $$\begin{cases} \deg_x(-v_1(v_1 + s) + u_1\delta_1) = 2 & \text{(2 eq.)} \\ v_1 + v_2 + s \equiv r\delta_1 \quad [u_2] & \text{(3 eq.)} \end{cases}$$

    where $s, \delta_1 \in k[x]$ with $\deg(s) = 2$ and $\deg(\delta_1) = 1$. Then

    $$E = (y - v_1)(y + v_1 + s) + u_1\delta_1$$

    Doubling

    compute $\omega_1 = (v_1^3 + v_1^2 h_1 + v_1 h_2 - f_3)/u_1$

    compute the inverse t_1 of ω_1 modulo u_1

    compute the remainder r of $(3v_1^2 + 2v_1 h_1 + h_2)t_1$ by u_1

    solve the linear equations given by the following conditions

    $$\begin{cases} \deg_x(-v_1(v_1 + s) + u_1\delta_1) = 2 & \text{(2 eq.)} \\ 2v_1 + s \equiv r\delta_1 \quad [u_1] & \text{(3 eq.)} \end{cases}$$

    where $s, \delta_1 \in k[x]$ with $\deg(s) = 2$ and $\deg(\delta_1) = 1$. Then

    $$E = (y - v_1)(y + v_1 + s) + u_1\delta_1$$

2. *Computation of the conic Q*

    compute $u' := Res^*(E, C, y)/(u_1 u_2)$

    compute the inverse α_1 of $t - s^2 - h_2 + sh_1$ modulo u'

    compute the remainder v' of $\alpha_1(st - th_1 - f_3)$ by u'

3. *Computation of $D_1 + D_2$*

    $v_{D_1+D_2} := v'$

    $u_{D_1+D_2} := ((v^3 + v^2 h_1 + vh_2 - f_3)/(u'))^*$

    $D_1 + D_2 = [u_{D_1+D_2}, v_{D_1+D_2}]$

For a polynomial g, we used the notation g^* to symbolize the quotient of g by its leading coefficient.

Remark. One may wonder about the special choice of the divisor D^∞. It was chosen such that the conic Q be of the form $y - v$. It thus gives directly the second part of the Mumford representation $[u, v]$ of the final divisor. Other choices of the points P_1^∞, P_2^∞ imply using an auxiliary conic to find the representation.

3.3. **Flex case.** This case is particulary interesting for fast computations in the Jacobian. Indeed, the expressions involved in Algorithm 1 are very similar to those in the Picard curves [8] case, and decrease the number of operations.

As in the tangent case, we can assume (after a linear transformation) that $l^\infty : z = 0$ is tangent at the flex $P_1^\infty = P_2^\infty = P_4^\infty = (0 : 1 : 0)$. An equation of C is

$$y^3 + h_1 y^2 + h_2 y = f_4,$$

where $h_1, h_2, f_4 \in k[x]$ with $\deg(h_2) \le 3, \deg(f_4) \le 4$. Moreover P_1^∞ is a flex point with tangent $z = 0$ if and only if $\deg(h_1) \le 1$ (consider the x-coordinates of the intersection $(l^\infty \cdot C)$).
In the same way as for the Lemma 1 we obtain

Lemma 2. *The cubic E is generically of the form*

$$y^2 + s \cdot y + t,$$

where s and t are polynomials in $k[x]$, with $\deg(s) \le 1$ and $\deg(t) \le 3$. The conic Q is of the form

$$y - v,$$

where $v \in k[x]$ and $\deg(v) = 2$.

Let $D_i = [u_i, v_i]$ in Mumford representation. As in the tangent case, division with rest of $y^2 + sy + t$ by $y - v_i$ gives

$$y^2 + sy + t = (y - v_i)(y + v_i + s) + r_i$$

where $r_i \in k[x]$ and $\deg(r_i) \le 4$. As the support of D_1 (resp. D_2) is contained in the support of $(C \cdot E)$ we have $r_i(x) = u_i(x)\delta_i(x)$. The computation of E reduces on finding the polynomials s and δ_1 in $k[x]$. The advantage is that s and δ_1 have now degree 1. Computations are thus a lot easier: the linear system in step 1 consists only of 4 equations, and consequently, the resultant $\text{res}(E, C, y)$ is easier to compute. In Algorithm 1 we just have to replace f_3 by f_4.

Furthermore, if $\text{char}(k) \ne 3$, we let $Y = y + h_1(x)/3$ and we can assume that C is of the following form:

$$Y^3 + h_2 Y = f_4,$$

with h_2 and f_4 as above. If in addition $\text{char}(k) \ne 2$, then we can assume that f_4 has no x^3 term.

3.4. **Comments on implementation.** We deal in this part with an optimized implementation in the case of the existence of a rational flex. To make the algorithm more efficient, we use the following well known methods:

(1) In order to reduce the number of field inversions, we use Montgomery's trick to compute simultaneous inversions. For the same reason, we compute almost inverses (using Bézout matrix), rather than inverses.

(2) We use either Karatsuba or Toom-Cook (in case $\text{char}(k) \neq 2, 3, 5$) trick to multiply two polynomials, and we compute only the coefficients we need in the algorithm. For instance, as we only need to know the quotient of the resultant of E and C by $u_1 u_2$, the degree ≤ 5 part of this resultant is irrelevant. Note that using Toom-Cook algorithm leads to divisions and multiplications by $2, 3$ and 5. These operations are not counted in the complexity since they are "easy".

(3) As explained in [2], one can try to use -2-adic expansion rather than usual 2-adic expansion, in order to save time for scalar multiplication. But this is only worthwhile if the computation of $-(D_1 + D_2)$ is easier than that of $D_1 + D_2$. This only happens in Theorem 1 if $P_1^\infty = P_2^\infty = P_4^\infty$. In that case (and only in that case), this leads to a saving of at least 10% for the computation of scalar multiples mD, assuming a ratio of $10 : 1$ for inversions and $2 : 3$ for squarings, in relation to multiplications. This saving is not yet included in our algorithm.

We give in Tables 1 and 2 the detailed and optimized operations in the case of existence of a rational flex and $\text{char}(k) > 5$. In that case, an addition requires $148M + 15SQ + 2I$ and a doubling $165M + 20SQ + 2I$. The interested reader can find a program in MAGMA at the following webpage:

http://www.math.uwaterloo.ca/~royono/Quartic.html

If C has a rational hyperflex and $\text{char}(k) > 5$, the nullity of an extra coefficient saves a couple of other operations. Addition then requires $131M + 14SQ + 2I$ and a doubling requires $148M + 19SQ + 2I$. Finally, note that the case of Picard curves has been handled in [8]. However, we point out that thanks to the new remarks made in this paper, we can actually reduce the cost for addition in the case of Picard curves to $116M + 14SQ + 2I$ and to $133M + 19SQ + 2I$ for doubling.

4. Examples

Fast additions can be useful in modern counting points algorithm and the two following examples are in this trend. The first example illustrates our algorithm in characteristic 2 and in the tangent case. Even without optimization, it is much faster than the existing (general) algorithm of MAGMA. The second case uses the optimized version with a flex.

4.1. **AGM-method.** In [21], a quasi-quadratic time algorithm for computing the Frobenius polynomial $\chi(X)$ of an ordinary non-hyperelliptic genus 3 curve C over $k = \mathbb{F}_{2^n}$ is described. However, the first part of the algorithm only gives $\chi(\pm X)$. Determining this sign can be done by checking for a generic degree 0 k-divisor D whether $\chi(1) \cdot D \sim 0$ or $\chi(-1) \cdot D \sim 0$.

Example 1. *Let C over $k = \mathbb{F}_{2^n}$ with $n = 100$, be defined by*

$$(\omega x^2 + (\omega^3 + 1)y^2 + \omega^2 z^2 + \omega^4 xy + (\omega^3 + \omega^2)xz + \omega^6 yz)^2 - xyz(x+y+z) = 0,$$

where the generator ω of k is a root of $(X^{101} - 1)/(X - 1)$. In 2 minutes,
[21] gives us

$$
\begin{aligned}
\chi_C(\pm X) = {} & X^6 + 377276036264709 \cdot X^5 + 3455351061169045838894227937403 \cdot X^4 \\
& + 929793021972276691307766666464616872277691871 \cdot X^3 \\
& + 3455351061169045838894227937403 \cdot 2^{100} \cdot X^2 \\
& + 377276036264709 \cdot 2^{200} \cdot X + 2^{300}.
\end{aligned}
$$

The line $z = 0$ is a bitangent at C at two rational points. We can now use the algorithm of Section 3.2 to prove in 4 seconds that the correct polynomial is $\chi(X)$. The same computation with MAGMA took 2 minutes.

4.2. 3-dimensional factors of $J^{new}(X_0(N))$.

Let f be a newform of $X_0(N)$. Following a construction due to Shimura, one may associate to this newform a factor of $J_0(N)$ (the Jacobian of $X_0(N)$), denoted A_f. If $\dim A_f \leq 3$, it is easy to determine whether it is the Jacobian of a 'modular' curve C_f or not (see for example [11] or [13]). In particular, if $\dim A_f = 3$, and if the curve C_f is non-hyperelliptic, an equation of C_f seems to be often given by linear relations in $S_2(f)^{\otimes 4}$. On the other hand, thanks to the Eichler-Shimura relation, fast computation of Hecke operators T_p leads to a fast determination of $\#\tilde{A}_f(\mathbb{F}_p)$ where $\tilde{A}_f = A_f \otimes \mathbb{F}_p$ for primes $p \nmid N$ (c.f. [10]). In order to check that one obtains the right equation for the curve, one can check that the group of rational points of its Jacobian has the expected order n by computing $n \cdot D$ for a random rational degree 0 divisor D.

Example 2. *We consider the modular curve $X_0(203)$. There is only one simple factor of dimension 3 in $J^{new}(X_0(203))$. We find one quartic relation between the associated cusp forms:*

$$C : y^4 - (x+3z)y^3 + y^2(x^2 - 3xz + 6z^2) + y(4xz^2 - 3z^3) - x^3 z + 3x^2 z^2 - 4xz^3 + 2z^4 = 0$$

We let now $p = 25033$. We denote $\tilde{C} = C \otimes \mathbb{F}_p$ and $\tilde{C}_f = C_f \otimes \mathbb{F}_p$. The computation of the characteristic polynomial of T_p leads to $\#Jac(\tilde{C}_f)(\mathbb{F}_p) = 15692826275509$, which is prime.
The curve $\tilde{C}$ has a rational flex. After a linear transformation, and by denoting new coordinates still by x, y, z, we have

$$
\begin{aligned}
\tilde{C} \quad : \quad & y^3 z + y^2(5057xz + 22616z^2) + y(6567x^3 + 18877x^2 z + 162xz^2 + 14333z^3) \\
= \quad & 8673x^4 + 24517x^3 z + 20295x^2 z^2 + 17815xz^3 + 3799z^4
\end{aligned}
$$

Choosing a random rational divisor, and computing its order, we may check in 0.14 seconds that, at least, $\#Jac(\tilde{C}_f)(\mathbb{F}_p)$ divides $\#Jac(\tilde{C})(\mathbb{F}_p)$.

5. Conclusion

We summarize here comparisons of the existing algorithms in the special case of genus 3 curves with a rational flex point. In particular, we did not include general algorithms for C_{ab} curves like in [14] since they only give asymptotic complexities.

We assume that $\text{char}(k) > 5$. Such a curve has a rational model $y^3 + h_2 y = f_4$ with $\deg h_2(x) \le 3$ and $\deg f_4(x) \le 4$. We sort out the methods according to the degree of h_2.

Operation		hyperelliptic of genus 3	$C_{3,4}$			'general' quartic $\deg(h_2) = 3$
			Picard	$\deg(h_2) = 1$	$\deg(h_2) = 2$	
Our	Add		2I+130M	2I+138M	2I+145M	2I+163M
Methods	Dbl		2I+152M	2I+160M	2I+167M	2I+185M
Previous	Add	I+70M [12]	2I+140M [4]	2I+147M [4]	2I+117M [22], 2I+150M [4]	
Work	Dbl	I+71M [12]	2I+164M [4]	2I+171M [4]	2I+129 M [22], 2I+174M [4]	

Some comments on this table:

- As far as we know, our algorithm is the fastest one for the 'general' genus 3 case.
- The algorithm [22] works also in characteristic 5 and is currently the fastest one for $C_{3,4}$ curves. Their method, which is a special case of [16] and [17], relies on a good choice of Riemann-Roch spaces and then has a geometric/algebraic flavor.
- In [4], the authors work in the function field of the curve, which allows them to use the tools from algorithmic number theory. In order to identify Jacobians and Class groups, they are restricted to work with a unique point at infinity.
- The algorithms [3] and [23] for Picard curves do not appear in this table as their point of view is different: they deal with the more general problem of reduction of divisors and they give only asymptotic complexity. We point out that a generalization of their method for C_{ab} curves based on geometric intersections, has been designed in [5].

6. Appendix

We show here how to compute the flexes of a plane algebraic curve $C : f(x_1, x_2, x_3) = 0$ of degree n over any algebraically closed field k of characteristic $p \ge 0$. Let P be a non-singular point of C. Recall that a point P is a *flex* if the intersection multiplicity at P of the tangent at P with C is greater than or equal to 3. This generalizes the definition given in Section 2.1. Non classical behaviors may appear when the characteristic divides $n-1$. For instance, there exist curves, called *funny curves*, for which all points are flexes (see for instance [15], where it is proved that a funny quartic is isomorphic to the Fermat quartic).

We are here interested in computational aspects of flexes. In characteristic 0, this is done by computing the Hessian.

Definition 1. *Denote by f_i the derivative of f with respect to x_i. We call the Hessian matrix of f the matrix $(f_{ij})_{i,j}$ and we call its determinant $H(f)$ the Hessian of f.*

The flexes are then the intersection points of the curve $H(f) = 0$ and C (see below Proposition 6). However, we shall see that this does not work

when p divides $2(n-1)$. In [1], Abhyankar gives a method to overcome the difficulty when $p \neq 2$.

Proposition 5 ([1])**.** *Assume that $p \neq 2$ and that $P = (a : b : 1) \in C$. Then P is a flex if and only if $h(a, b) = 0$ with*

$$h(x_1, x_2) = \begin{vmatrix} f(x_1, x_2, 1) & f_1(x_1, x_2, 1) & f_2(x_1, x_2, 1) \\ f_1(x_1, x_2, 1) & f_{11}(x_1, x_2, 1) & f_{12}(x_1, x_2, 1) \\ f_2(x_1, x_2, 1) & f_{21}(x_1, x_2, 1) & f_{22}(x_1, x_2, 1) \end{vmatrix}.$$

We present here a method which works in any characteristic. We will need the following lemmas.

Lemma 3. *Let $g \in GL_3(k)$ be a linear transformation. Then $H(f \circ g^{-1}) = (\det g)^2 \cdot H(f) \circ g^{-1}$.*

Proof. Apply the chain rule. □

Lemma 4. $x_1^2 H(f) = \begin{vmatrix} n(n-1)f & (n-1)f_2 & (n-1)f_3 \\ (n-1)f_2 & f_{22} & f_{23} \\ (n-1)f_3 & f_{23} & f_{33} \end{vmatrix}$

Proof. Apply twice the Euler's formula $x_1 f_1 + x_2 f_2 + x_3 f_3 = (\deg f)f$. See for example [20]. □

If $f = 0$ is an equation of C of degree $n \geq 3$, then there exists a linear transformation g which sends a non-singular point $P = (p_1 : p_2 : p_3)$ on $(1 : 0 : 0)$ and its tangent to the line $x_3 = 0$. Then in affine coordinates

$$(1) \qquad f \circ g^{-1} = x_2 + rx_2^2 + sx_2 x_3 + tx_3^2 + R(x_2, x_3)$$

and R has only terms of degree greater or equal to 3. Then P is a flex if and only if $r = 0$.

Proposition 6. *Suppose that p does not divide $2(n-1)$. Then P is a flex if and only if $H(f)(P) = 0$.*

Proof. Suppose that the x_1-coordinate of P is not 0 (otherwise do the same proof with an other coordinate). We have

$$(x_1^2 H(f) \circ g^{-1})(g(P)) = (\det g)^{-2}(x_1^2 H(f \circ g^{-1}))(g(P))$$

by Lemma 3 and because the $x_i x_j$ $(i, j \neq 1)$ terms in $(x_1^2) \circ g^{-1}$ are 0 at $g(P) = (1 : 0 : 0)$. Then by Lemma 4 and the form of $f \circ g^{-1}$

$$(x_1^2 H(f))(P) = -(\det g)^{-2} 2(n-1)^2 r.$$

So $H(f)(P) = 0$ if and only if $r = 0$ (i.e. P is a flex).

□

The proof shows also that this method can fail if p divides $2(n-1)$. We then suggest the following strategy. Denote K a complete local field of characteristic 0, $\mathcal{O}$ its ring of integers, $\mathcal{M}$ its maximal ideal such that $\mathcal{O}/\mathcal{M} \simeq k$ ($\mathcal{O}$ may be the ring of Witt vectors of k).

Proposition 7. *Let $\mathcal{C}/\mathcal{O}$ be a model of C given by a polynomial $F \in \mathcal{O}[X_1, X_2, X_3]$. We denote $\overline{H}$ the polynomial*

$$\overline{H} = \frac{X_1^2 H(F) - n(n-1)F(F_{22}F_{33} - F_{23}^2)}{2(n-1)^2}.$$

Then $\overline{H}$ is in $\mathcal{O}[X_1, X_2, X_3]$. We call $\overline{h}$ its reduction modulo $\mathcal{M}$.
Let $P = (1 : a : b) \in C$ be a non-singular point. The point P is a flex if and only if $\overline{h}(1, a, b) = 0$.

Proof. First we prove that $\overline{H}$ is in $\mathcal{O}[X_1, X_2, X_3]$. By Lemma 4,

$$X_1^2 H(F) - n(n-1)F(F_{22}F_{33} - F_{23}^2) = (n-1)^2(2F_2F_3F_{23} - F_2^2 F_{33} - F_3^2 F_{22}).$$

So $2(n-1)^2$ divides $X_1^2 H(F) - n(n-1)F(F_{22}F_{33} - F_{23}^2)$.

Since P is non-singular, there exists $\mathcal{P} = (1 : A : B) \in C(\mathcal{O})$ lifting P. Let $g \in \mathrm{GL}_3(\mathcal{O})$ a linear transformation that maps $\mathcal{P}$ on $(1 : 0 : 0)$ with tangent $X_3 = 0$. The reduction of this point is a flex if and only if the corresponding r (of equation (1)) is in $\mathcal{M}$. Now

$$\overline{H}(\mathcal{P}) = \frac{(X_1^2 H(F))(\mathcal{P})}{2(n-1)^2} = -\deg(g)^2 \cdot r$$

by the computations of Proposition 6. So P is a flex if and only if $\overline{h}(1, a, b) = 0$. $\qquad\square$

Acknowledgment. *The formula*

$$(2F_2F_3F_{23} - F_2^2 F_{33} - F_3^2 F_{22})$$

TABLE 1. **Addition,** $\deg u_1 = \deg u_2 = 3$

Input	$D_1 = [u_1, v_1]$ and $D_2 = [u_2, v_2]$	
	$u_i = x^3 + u_{i2}x^2 + u_{i1}x + u_{i0}, v_i = v_{i2}x^2 + v_{i1}x + v_{i0}$	
	$C : y^3 + h(x)y - f(x) = 0$ with	
	$h(x) := h_3x^3 + h_2x^2 + h_1x + h_0, \; f(x) := x^4 + f_2x^2 + f_1x + f_0$	
Output	$D = [u_{D_1+D_2}, v_{D_1+D_2}] = D_1 + D_2$ with	
	$u_{D_1+D_2} = x^3 + u_2x^2 + u_1x + u_0$	
	$v_{D_1+D_2} = v_2x^2 + v_1x + v_0$	
Step	Expression	Operations
1.1	compute the inverse t_1 of $v_1 - v_2$ modulo u_2	13M+2SQ
	$a_1 = (v_{12}-v_{22})u_{22} - (v_{11}-v_{21}), a_2 = (v_{12}-v_{22})^2, a_3 = a_2u_{20} - a_1(v_{10}-v_{20});$	
	$a_4 = a_2(u_{22}+u_{21}+u_{20}+1) - (v_{12}-v_{22}+a_1)(v_{12}+v_{11}+v_{10}-(v_{22}+v_{21}+v_{20})) - a_3;$	
	$a_5 = a_4(v_{12}-v_{22}), a_6 = a_4(v_{11}-v_{21}) - a_3(v_{12}-v_{22});$	
	$a_7 = a_4^2, res_1 = a_7(v_{10}-v_{20}) - a_6a_3, t_{10} = a_1a_6, t_{12} = (v_{12}-v_{22})a_5;$	
	$t_{11} = (a_1+v_{12}-v_{22})(a_6+a_5) - (t_{10}+t_{12}), t_{10} = t_{10} + a_7;$	
	$\qquad\qquad t_1 = t_{12}x^2 + t_{11}x + t_{10}$	
1.2	compute the remainder r of $(u_1 - u_2)t_1$ by u_2	9M
	$b_1 = (u_{12}+u_{11}+u_{10} - (u_{22}+u_{21}+u_{20}))(t_{12}+t_{11}+t_{10});$	
	$b_2 = (u_{12}-u_{11}+u_{10} - (u_{22}-u_{21}+u_{20}))(t_{12}-t_{11}+t_{10});$	
	$b_3 = (4(u_{12}-u_{22}) + 2(u_{11}-u_{21}) + u_{10}-u_{20})(4t_{12}+2t_{11}+t_{10});$	
	$b_4 = (u_{12}-u_{22})t_{12}, b_5 = (u_{10}-u_{20})t_{10}, b_6 = (b_1+b_2)/2 - (b_5+b_4);$	
	$b_7 = ((b_3+b_2-b_1-b_5)/2 - 2(4b_4+b_6))/3, b_8 = b_1 - (b_5+b_6+b_7+b_4);$	
	$b_9 = b_7 - b_4u_{22}, r_2 = b_5 - b_9u_{20};$	
	$b_{10} = b_4+b_7+b_6+b_8+b_5 - (b_9+b_4)(u_{22}+u_{21}+u_{20}+1);$	
	$r_1 = (b_{10} - (b_4+b_6+b_5 - (b_7+b_8) - (b_9-b_4)(u_{22}-u_{21}+u_{20}-1)))/2;$	
	$r_0 = b_{10} - (r_2+r_1);$	
	$\qquad\qquad r = r_0x^2 + r_1x + r_2$	
1.3	compute the cubic $E = y^2 + sy + t$	39M+3SQ+I
	$c_1 = v_{12}^2, c_2 = r_0c_1, c_3 = res_1 \cdot (v_{12}+v_{22}) - (r_1c_1) + (c_2u_{22}), c_4 = c_3 \cdot res_1;$	
	$c_5 = res_1 \cdot r_0, c_6 = r_0c_2, c_7 = r_2c_3 - (c_6u_{20}) - c_5(v_{10}+v_{20});$	
	$c_8 = (r_0+r_1+r_2)(c_2+c_3) - c_6(1 + (u_{22}+u_{21}+u_{20})) - c_5(v_{22}+v_{21}+v_{20} + v_{12}+v_{11}+v_{10}) - c_7;$	
	$c_9 = c_4 + u_{12}c_5c_1 - v_{12}(c_8 + 2c_5v_{11}), c_{10} = c_5c_9, c_{11} = c_5^2;$	
*1	$c_{12} = c_9^2, c_{13} = c_{12} + h_3(-2c_{10}+h_3c_{11}), inv_1 = (c_{10}c_{13})^{-1}, c_{14} = c_{13} \cdot inv_1;$	(7M+SQ+I)
	$c_{15} = c_9c_{14}, c_{16} = c_{12} \cdot inv_1 \cdot c_{10};$	
	$s_0 = c_7c_{15}, s_1 = c_8c_{15}, c_{17} = c_4c_{15};$	
	$c_{18} = (1+u_{12}+u_{11}+u_{10})(c_1+c_{17}) - (v_{12}+v_{11}+v_{10})(v_{12}+v_{11}+v_{10}+s_1+s_0);$	
	$t_3 = c_9c_{15}, t_0 = u_{10}c_{17} - v_{10}(v_{10}+s_0);$	
	$t_2 = (c_{18} + (-1+u_{12}-u_{11}+u_{10})(-c_1+c_{17}) - (v_{12}-v_{11}+v_{10})(v_{12}-v_{11} + v_{10}-s_1+s_0))/2 - t_0;$	
	$t_1 = c_{18} - (t_0+t_2+t_3), k_1 = c_{11}c_{14}, c_{19} = t_0k_1, c_{20} = t_1k_1, c_{21} = t_2k_1;$	
	$\qquad\qquad E = y^2 + (s_1x+s_0)y + t_3x^3 + t_2x^2 + t_1x + t_0$	
2.1	compute $res(E, C, y)$ and $u' := res(E,C,y)^*/(u_1u_2)$	37M+5SQ
	$d_0 = c_{21}^2, d_1 = 3c_{21}, d_2 = 3(c_{20}+d_0), d_3 = c_{21}(6c_{20}+d_0) + 3c_{19};$	
	$d_4 = s_1^2, d_5 = s_0^2, d_6 = (s_1+s_0)^2 - (d_4+d_5), d_7 = (s_1+s_0)(t_3+t_2+t_1+t_0);$	
	$d_8 = (s_0-s_1)(t_2+t_0 - (t_3+t_1)), d_9 = (2s_1+s_0)(8t_3+4t_2+2t_1+t_0);$	
	$d_{10} = s_1t_3, d_{11} = s_0t_0, d_{12} = -(d_{11}+d_{10}) + (d_7+d_8)/2;$	
	$d_{13} = -2d_{10} + (d_{11}-d_7 + (d_9-d_8)/3)/2, d_{14} = d_7 - (d_{11}+d_{12}+d_{13}+d_{10});$	
	$d_{15} = s_1d_4, d_{16} = 3d_4s_0, d_{17} = 1 - 3d_{10}, d_{18} = d_{15} - 3d_{13};$	
	$d_{19} = f_2 + d_{16} + (1 - 3d_{10})f_2 - 3d_{12};$	
*2	$d_{20} = (t_3+t_2+t_1+t_0)(h_3+h_2+h_1+h_0 + d_4+d_6+d_5 - 2(t_3+t_2+t_1+t_0));$	(15M)
	$d_{21} = (-t_3+t_2-t_1+t_0)(2(t_3-t_2+t_1-t_0) - h_3+h_2-h_1+h_0 + d_4-d_6+d_5);$	
	$d_{22} = (8t_3+4t_2+2t_1+t_0)(8(-2t_3+h_3) + 4(d_4-2t_2+h_2) + 2(d_6-2t_1 + h_1) + d_5 - 2t_0 + h_0);$	

	$d_{23} = (-8t_3 + 4t_2 - 2t_1 + t_0)(-8(-2t_3 + h_3) + 4(d_4 - 2t_2 + h_2) - 2(d_6 - 2t_1 + h_1) + d_5 - 2t_0 + h_0);$ $d_{24} = (27t_3 + 9t_2 + 3t_1 + t_0)(27(-2t_3 + h_3) + 9(d_4 - 2t_2 + h_2) + 3(d_6 - 2t_1 + h_1) + d_5 - 2t_0 + h_0);$ $d_{25} = t_0(d_5 - 2t_0 + h_0), d_{26} = t_3(-2t_3 + h_3), d_{32} = f_2 s_1;$ $d_{27} = -5d_{26} + ((-(d_{20} + d_{21}) + (3d_{25} + (d_{23} + d_{22})/2)/2)/2)/3;$ $d_{28} = 15d_{26} + (((5d_{25} - 7d_{20} + (-d_{24} + 7d_{22} - d_{23} - d_{21})/2)/2)/2)/3;$ $d_{29} = -3d_{26} + (((d_{20} - d_{25} + (d_{21} - d_{22} + (d_{24} - d_{23})/5)/2)/2)/2)/3;$ $d_{33} = (h_3 + h_2 + h_1 + h_0)(d_{26} + d_{29} + d_{27} + d_{28} + s_1 + s_0 + d_{32});$ $d_{34} = (-h_3 + h_2 - h_1 + h_0)(-d_{26} + d_{29} - d_{27} + d_{28} + s_1 - s_0 + d_{32});$ $d_{35} = (8h_3 + 4h_2 + 2h_1 + h_0)(8d_{26} + 4(d_{29} + s_1) + 2(d_{27} + s_0) + d_{28} + d_{32});$ $d_{36} = (-8h_3 + 4h_2 - 2h_1 + h_0)(-8d_{26} + 4(d_{29} + s_1) - 2(d_{27} + s_0) + d_{28} + d_{32});$ $d_{37} = (27h_3 + 9h_2 + 3h_1 + h_0)(27d_{26} + 9(d_{29} + s_1) + 3(d_{27} + s_0) + d_{28} + d_{32});$ $d_{38} = h_0(d_{28} + d_{32}), d_{44} = h_3 d_{26};$ $d_{42} = -5d_{44} + ((-(d_{33} + d_{34}) + (3d_{38} + (d_{36} + d_{35})/2)/2)/2)/3;$ $d_{41} = 15d_{44} + (((5d_{38} - 7d_{33} + (-d_{37} + 7d_{35} - d_{36} - d_{34})/2)/2)/2)/3;$ $d_{43} = -3d_{44} + (((d_{33} - d_{38} + (d_{34} - d_{35} + (d_{37} - d_{36})/5)/2)/2)/2)/3;$ $d_{40} = (d_{33} + d_{34})/2 - (d_{38} + d_{42} + d_{44});$ $d_{39} = d_{33} - (d_{38} + d_{40} + d_{41} + d_{42} + d_{43} + d_{44});$	
	$d_{45} = k_1^3, d_{46} = d_{45}(d_{19} + d_{41}) + d_3, d_{47} = d_{45}(d_{18} + d_{42}) + d_2;$ $d_{48} = d_{45}(d_{17} + d_{43}) + d_1;$	
$*3$	$d_{46} = d_{46}c_{16}, d_{47} = d_{47}c_{16}, d_{48} = d_{48}c_{16};$	(3M)
	$d_{49} = u_{12} + u_{22}, d_{50} = u_{21} + u_{11} + u_{12}u_{22};$ $d_{51} = u_{20} + u_{10} + u_{12}u_{21} + u_{11}u_{22}, u_2' = d_{48} - d_{49};$ $u_1' = d_{47} - d_{50} - d_{49}u_2', u_0' = -d_{49}u_1' + d_{46} - d_{51} - d_{50}(d_{48} - d_{49});$ $u' = x^3 + u_2'x^2 + u_1'x + u_0'$	
2.2	compute the inverse α_1 of $t - s^2 - h$ modulo u' $g_1 = t_3 - h_3, g_0 = g_1(1 + u_2' + u_1' + u_0'), g_2 = t_0 - (d_5 + h_0 + g_1 u_0');$ $g_3 = t_3 + t_2 + t_1 + t_0 - (h_3 + h_2 + h_1 + h_0 + d_4 + d_6 + d_5 + g_0);$ $g_5 = (t_3 + t_2 + t_1 + t_0 - (h_3 + h_2 + h_1 + h_0 + d_4 + d_6 + d_5 + g_0) - (-t_3 + t_2 - t_1 + t_0 + h_3 - h_2 + h_1 - h_0 - d_4 + d_6 - d_5 - g_1(-1 + u_2' - u_1' + u_0')))/2;$ $g_6 = g_3 - g_5 - g_2, g_7 = g_6 u_2' - g_5, g_8 = g_6^2, g_{10} = g_8 u_0' - g_7 g_2;$ $g_{11} = g_8(1 + u_2' + u_1' + u_0') - (g_6 + g_7)(g_6 + g_5 + g_2) - g_{10}, g_{12} = g_{11}g_6;$ $g_{13} = g_{11}g_5 - g_{10}g_6, g_9 = g_{11}^2, res_2 = g_9 g_2 - g_{13}g_{10}, \alpha_{10} = g_7 g_{13};$ $\alpha_{12} = g_6 g_{12}, \alpha_{11} = (g_6 + g_7)(g_{12} + g_{13}) - \alpha_{10} - \alpha_{12}, \alpha_{10} = \alpha_{10} + g_9;$ $\alpha_1 = \alpha_{12}x^2 + \alpha_{11}x + \alpha_{10}$	16M+2SQ
2.3	compute the remainder v of $\alpha_1(st - f_4)$ by u' $i_1 = d_{10} - 1, i_2 = d_{13} - (d_{10} - 1)u_2', i_3 = d_{11} - f_0 - i_2 u_0';$ $i_4 = d_{10} + d_{13} + d_{12} + d_{14} + d_{11} - (1 + f_2 + f_1 + f_0) - (i_2 + i_1)(u_2' + u_1' + u_0' + 1);$ $i_5 = (i_4 - ((d_{10} - d_{13} + d_{12} - d_{14} + d_{11} - 1 - f_2 + f_1 - f_0) - (i_2 - i_1)(u_2' - u_1' + u_0' - 1)))/2;$ $i_6 = i_4 - i_3 - i_5, i_7 = (i_6 + i_5 + i_3)(\alpha_{12} + \alpha_{11} + \alpha_{10}), i_9 = i_6 \alpha_{12}, i_{10} = i_3 \alpha_{10};$ $i_8 = (i_6 - i_5 + i_3)(\alpha_{12} - \alpha_{11} + \alpha_{10}), i_{11} = (i_7 + i_8)/2 - (i_{10} + i_9);$ $i_{12} = (((4i_6 + 2i_5 + i_3)(4\alpha_{12} + 2\alpha_{11} + \alpha_{10}) - i_7 + i_8 - i_{10})/2 - 2(4i_9 + i_{11}))/3;$ $i_{13} = i_7 - (i_{10} + i_{11} + i_{12} + i_9), i_{14} = i_9, i_{15} = i_{12} - i_9 u_2', i_{16} = i_{10} - i_{15}u_0';$ $i_{17} = (i_9 + i_{12} + i_{11} + i_{13} + i_{10}) - (i_{15} + i_{14})(u_2' + u_1' + u_0' + 1);$ $i_{18} = (i_{17} - (i_9 - i_{12} + i_{11} - i_{13} + i_{10}) + (i_{15} - i_{14})(u_2' - u_1' + u_0' - 1))/2;$ $i_{19} = i_{17} - i_{16} - i_{18}, inv_2 = (res_2 \cdot i_{19})^{-1}, i_{20} = inv_2 \cdot i_{19};$ $v_0 = i_{20}i_{16}, v_1 = i_{20}i_{18}, v_2 = i_{20}i_{19};$ $v = v_2 x^2 + v_1 x + v_0$	18M+I
3	compute $u := u_{D_1 + D_2}$ $j_1 = inv_2 \cdot res_2^2, j_2 = j_1^3, j_3 = j_1 v_1, j_4 = j_3^2, j_5 = j_1 v_0, j_6 = j_3(j_4 + 6j_5);$	16M+3SQ
$*4$	$j_7 = (v_2 + v_1 + v_0)(h_3 + h_2 + h_1), j_8 = (v_2 - v_1 + v_0)(h_3 - h_2 + h_1), j_9 = v_2 h_3;$ $j_{10} = v_0 h_1, j_{11} = (j_7 + j_8)/2 - (j_{10} + j_9), j_{12} = 3j_3 + j_2 j_9, j_{14} = j_6 + j_2 j_{11};$ $j_{13} = 3(j_5 + j_4) - j_2 + j_2((((4v_2 + 2v_1 + v_0)(4h_3 + 2h_2 + h_1) - j_7 + j_8 - j_{10})/2 - 2(4j_9 + j_{11}))/3);$	(8M)
	$u_2 = j_{12} - u_2', u_1 = j_{13} - u_1' - u_2'u_2, u_0 = -u_2'u_1 + j_{14} - u_0' - u_1'(j_{12} - u_2');$ $u = x^3 + u_2 x^2 + u_1 x + u_0$	
total		148M, 15SQ, 2I

TABLE 2. **Doubling,** $\deg u_1 = 3$

Input	$D_1 = [u_1, v_1]$
	$u_1 = x^3 + u_{12}x^2 + u_{11}x + u_{10}, \ v_1 = v_{12}x^2 + v_{11}x + v_{10}$
	$C : y^3 + h(x)y - f(x) = 0$ with
	$h(x) := h_3x^3 + h_2x^2 + h_1x + h_0, \ f(x) := x^4 + f_2x^2 + f_1x + f_0$
Output	$D = [u_{2D_1}, v_{2D_1}] = 2D_1$ with
	$u_{2D_1} = x^3 + u_2x^2 + u_1x + u_0$
	$v_{2D_1} = v_2x^2 + v_1x + v_0$

Step	Expression	Operations
1.1	compute w_1 such that $u_1w_1 = v_1^3 + h(x)v_1 - f(x)$	12M+5SQ
	$l_1 = (v_{12} + v_{11} + v_{10})^2, l_2 = (v_{12} - v_{11} + v_{10})^2, l_3 = v_{12}^2, l_4 = v_{10}^2;$	
	$l_5 = (l_1 + l_2)/2 - (l_4 + l_3);$	
	$l_6 = (((4v_{12} + 2v_{11} + v_{10})^2 - l_1 + l_2 - l_4)/2 - 2(4l_3 + l_5))/3;$	
	$l_7 = l_1 - (l_4 + l_5 + l_6 + l_3), l_8 = (v_{12} + v_{11} + v_{10})(l_3 + l_6 + l_5 + l_7 + h_3 + h_2 + h_1);$	
	$l_9 = (v_{12} - v_{11} + v_{10})(-l_3 + l_6 + h_3 - (l_5 + h_2) + l_7 + h_1);$	
	$l_{10} = (4v_{12} + 2v_{11} + v_{10})(8l_3 + 4(l_6 + h_3) + 2(l_5 + h_2) + l_7 + h_1);$	
	$l_{11} = (4v_{12} - 2v_{11} + v_{10})(-8l_3 + 4(l_6 + h_3) - 2(l_5 + h_2) + l_7 + h_1);$	
	$l_{12} = v_{10}(l_7 + h_1), l_{13} = v_{12}l_3, l_{14} = -5l_{13} + ((l_9 - l_8 + (l_{10} - l_{11})/2)/2)/3;$	
	$l_{15} = ((-(l_8 + l_9) + (3l_{12} + (l_{10} + l_{11})/2)/2)/2)/3;$	
	$l_{16} = (l_8 + l_9)/2 - (l_{12} + l_{15}), l_{14} = l_{14} - 1, w_{13} = l_{13}, w_{12} = l_{15} - w_{13}u_{12};$	
	$w_{11} = l_{14} - w_{13}u_{11} - w_{12}u_{12}, w_{10} = l_{16} - w_{13}u_{10} - w_{12}u_{11} - w_{11}u_{12};$	
	$\qquad w_1 = w_{13}x^3 + w_{12}x^2 + w_{11}x + w_{10}$	
1.2	compute the inverse t_1 of w_1 modulo u_1	16M+2SQ
	$a_1 = w_{13}, a_2 = w_{10} - a_1u_{10};$	
	$a_3 = w_{13} + w_{12} + w_{11} + w_{10} - a_1(1 + u_{12} + u_{11} + u_{10});$	
	$a_4 = (a_3 - (-w_{13} + w_{12} - w_{11} + w_{10} - a_1(-1 + u_{12} - u_{11} + u_{10})))/2;$	
	$a_5 = a_3 - a_4 - a_2, a_6 = a_5u_{12} - a_4, a_7 = a_5^2, a_8 = a_7u_{10} - a_6a_2;$	
	$a_9 = a_7(1 + u_{12} + u_{11} + u_{10}) - (a_5 + a_6)(a_5 + a_4 + a_2) - a_8, a_{10} = a_9a_5;$	
	$a_{11} = a_9a_4 - a_8a_5, a_7 = a_9^2, res_1 = a_7a_2 - a_{11}a_8, t_{10} = a_6a_{11};$	
	$t_{12} = a_5a_{10}, t_{11} = (a_5 + a_6)(a_{10} + a_{11}) - t_{10} - t_{12}, t_{10} = t_{10} + a_7;$	
	$\qquad t_1 = t_{12}x^2 + t_{11}x + t_{10}$	
1.3	compute the remainder r of $(3v_1^2 + h)t_1$ by u_1	13M
	$b_1 = 3l_6 + h_3 - 3l_3u_{12}, b_2 = 3l_4 + h_0 - b_1u_{10};$	
	$b_3 = (3l_3 + 3l_6 + h_3 + 3l_5 + h_2 + 3l_7 + h_1 + 3l_4 + h_0) - (b_1 + 3l_3)(u_{12} + u_{11} + u_{10} + 1);$	
	$b_4 = (b_3 - ((3l_3 - (3l_6 + h_3) + 3l_5 + h_2 - (3l_7 + h_1) + 3l_4 + h_0) - (b_1 - 3l_3)(u_{12} -$	
	$u_{11} + u_{10} - 1)))/2;$	
	$b_5 = b_3 - b_2 - b_4, b_6 = (b_5 + b_4 + b_2)(t_{12} + t_{11} + t_{10});$	
	$b_7 = (b_5 - b_4 + b_2)(t_{12} - t_{11} + t_{10}), b_8 = b_5t_{12}, b_9 = b_2t_{10};$	
	$b_{10} = (b_6 + b_7)/2 - (b_9 + b_8);$	
	$b_{11} = (((4b_5 + 2b_4 + b_2)(4t_{12} + 2t_{11} + t_{10}) - b_6 + b_7 - b_9)/2 - 2(4b_8 + b_{10}))/3;$	
	$b_{12} = b_6 - (b_9 + b_{10} + b_{11} + b_8), b_{13} = b_{11} - b_8u_{12}, r_2 = b_9 - b_{13}u_{10};$	
	$b_{14} = (b_8 + b_{11} + b_{10} + b_{12} + b_9) - (b_{13} + b_8)(u_{12} + u_{11} + u_{10} + 1);$	
	$r_1 = (b_{14} - (b_8 + b_{10} + b_9) + (b_{11} + b_{12}) + (b_{13} - b_8)(u_{12} - u_{11} + u_{10} - 1))/2;$	
	$r_0 = b_{14} - (r_2 + r_1);$	
	$\qquad r = r_0x^2 + r_1x + r_2$	
1.4	compute the cubic $E = y^2 + sy + t$	39M+2SQ+I
	$c_1 = l_3, c_2 = r_0c_1, c_3 = 2res_1 \cdot v_{12} - (r_1c_1 - c_2u_{12}), c_4 = c_3 \cdot res_1, c_5 = res_1 \cdot r_0;$	
	$c_6 = r_0c_2, c_7 = r_2c_3 - c_6u_{10} - 2c_5v_{10};$	
	$c_8 = (r_0 + r_1 + r_2)(c_2 + c_3) - c_6(1 + u_{12} + u_{11} + u_{10}) - 2c_5(v_{12} + v_{11} + v_{10}) - c_7;$	
	$c_9 = c_4 + u_{12}c_5c_1 - v_{12}(c_8 + 2c_5v_{11}), c_{10} = c_5c_9, c_{11} = c_5^2;$	
*1	$c_{12} = c_9^2, c_{13} = c_{12} + h_3(-2c_{10} + h_3c_{11}), inv_1 = (c_{10}c_{13})^{-1}, c_{14} = c_{13} \cdot inv_1;$	(7M+SQ+I)
	$c_{15} = c_9c_{14}, c_{16} = c_{12} \cdot inv_1 \cdot c_{10};$	
	$s_0 = c_7c_{15}, s_1 = c_8c_{15}, c_{17} = c_4c_{15};$	
	$c_{18} = (1 + u_{12} + u_{11} + u_{10})(c_1 + c_{17}) - (v_{12} + v_{11} + v_{10})(v_{12} + v_{11} + v_{10} + s_1 + s_0);$	
	$t_3 = c_9c_{15}, t_0 = u_{10}c_{17} - v_{10}(v_{10} + s_0);$	
	$t_2 = (c_{18} + (-1 + u_{12} - u_{11} + u_{10})(-c_1 + c_{17}) - (v_{12} - v_{11} + v_{10})(v_{12} - v_{11} +$	
	$v_{10} - s_1 + s_0))/2 - t_0;$	
	$t_1 = c_{18} - (t_0 + t_2 + t_3), k_1 = c_{11}c_{14}, c_{19} = t_0k_1, c_{20} = t_1k_1, c_{21} = t_2k_1;$	
	$\qquad E = y^2 + (s_1x + s_0)y + t_3x^3 + t_2x^2 + t_1x + t_0$	

2.1	compute $res(E,C,y)$ and $u' := res(E,C,y)^*/(u_1 u_2)$	35M+6SQ
	$d_0 = c_{21}^2$, $d_1 = 3c_{21}$, $d_2 = 3(c_{20} + d_0)$, $d_3 = c_{21}(6c_{20} + d_0) + 3c_{19}$; $d_4 = s_1^2$, $d_5 = s_0^2$, $d_6 = (s_1 + s_0)^2 - (d_4 + d_5)$, $d_7 = (s_1 + s_0)(t_3 + t_2 + t_1 + t_0)$; $d_8 = (s_0 - s_1)(t_2 + t_0 - (t_3 + t_1))$, $d_9 = (2s_1 + s_0)(8t_3 + 4t_2 + 2t_1 + t_0)$; $d_{10} = s_1 t_3$, $d_{11} = s_0 t_0$, $d_{12} = -(d_{11} + d_{10}) + (d_7 + d_8)/2$; $d_{13} = -2d_{10} + (d_{11} - d_7 + (d_9 - d_8)/3)/2$, $d_{14} = d_7 - (d_{11} + d_{12} + d_{13} + d_{10})$; $d_{15} = s_1 d_4$, $d_{16} = 3d_4 s_0$, $d_{17} = 1 - 3d_{10}$, $d_{18} = d_{15} - 3d_{13}$; $d_{19} = f_2 + d_{16} + (1 - 3d_{10})f_2 - 3d_{12}$;	
*2	$d_{20} = (t_3 + t_2 + t_1 + t_0)(h_3 + h_2 + h_1 + h_0 + d_4 + d_6 + d_5 - 2(t_3 + t_2 + t_1 + t_0))$; $d_{21} = (-t_3 + t_2 - t_1 + t_0)(2(t_3 - t_2 + t_1 - t_0) - h_3 + h_2 - h_1 + h_0 + d_4 - d_6 + d_5)$; $d_{22} = (8t_3 + 4t_2 + 2t_1 + t_0)(8(-2t_3 + h_3) + 4(d_4 - 2t_2 + h_2) + 2(d_6 - 2t_1 + h_1) + d_5 - 2t_0 + h_0)$; $d_{23} = (-8t_3 + 4t_2 - 2t_1 + t_0)(-8(-2t_3 + h_3) + 4(d_4 - 2t_2 + h_2) - 2(d_6 - 2t_1 + h_1) + d_5 - 2t_0 + h_0)$; $d_{24} = (27t_3 + 9t_2 + 3t_1 + t_0)(27(-2t_3 + h_3) + 9(d_4 - 2t_2 + h_2) + 3(d_6 - 2t_1 + h_1) + d_5 - 2t_0 + h_0)$; $d_{25} = t_0(d_5 - 2t_0 + h_0)$, $d_{26} = t_3(-2t_3 + h_3)$, $d_{32} = f_2 s_1$; $d_{27} = -5d_{26} + ((-(d_{20} + d_{21}) + (3d_{25} + (d_{23} + d_{22})/2)/2)/2)/3$; $d_{28} = 15d_{26} + (((5d_{25} - 7d_{20} + (-d_{24} + 7d_{22} - d_{23} - d_{21})/2)/2)/2)/3$; $d_{29} = -3d_{26} + (((d_{20} - d_{25} + (d_{21} - d_{22} + (d_{24} - d_{23})/5)/2)/2)/2)/3$; $d_{33} = (h_3 + h_2 + h_1 + h_0)(d_{26} + d_{29} + d_{27} + d_{28} + s_1 + s_0 + d_{32})$; $d_{34} = (-h_3 + h_2 - h_1 + h_0)(-d_{26} + d_{29} - d_{27} + d_{28} + s_1 - s_0 + d_{32})$; $d_{35} = (8h_3 + 4h_2 + 2h_1 + h_0)(8d_{26} + 4(d_{29} + s_1) + 2(d_{27} + s_0) + d_{28} + d_{32})$; $d_{36} = (-8h_3 + 4h_2 - 2h_1 + h_0)(-8d_{26} + 4(d_{29} + s_1) - 2(d_{27} + s_0) + d_{28} + d_{32})$; $d_{37} = (27h_3 + 9h_2 + 3h_1 + h_0)(27d_{26} + 9(d_{29} + s_1) + 3(d_{27} + s_0) + d_{28} + d_{32})$; $d_{38} = h_0(d_{28} + d_{32})$, $d_{44} = h_3 d_{26}$; $d_{42} = -5d_{44} + ((-(d_{33} + d_{34}) + (3d_{38} + (d_{36} + d_{35})/2)/2)/2)/3$; $d_{41} = 15d_{44} + (((5d_{38} - 7d_{33} + (-d_{37} + 7d_{35} - d_{36} - d_{34})/2)/2)/2)/3$; $d_{43} = -3d_{44} + (((d_{33} - d_{38} + (d_{34} - d_{35} + (d_{37} - d_{36})/5)/2)/2)/2)/3$; $d_{40} = (d_{33} + d_{34})/2 - (d_{38} + d_{42} + d_{44})$; $d_{39} = d_{33} - (d_{38} + d_{40} + d_{41} + d_{42} + d_{43} + d_{44})$;	(15M)
	$d_{45} = k_1^3$, $d_{46} = d_{45}(d_{19} + d_{41}) + d_3$, $d_{47} = d_{45}(d_{18} + d_{42}) + d_2$; $d_{48} = d_{45}(d_{17} + d_{43}) + d_1$;	
*3	$d_{46} = d_{46}c_{16}$, $d_{47} = d_{47}c_{16}$, $d_{48} = d_{48}c_{16}$;	(3M)
	$d_{49} = 2u_{12}$, $d_{50} = 2u_{11} + u_{12}^2$, $d_{51} = 2u_{10} + 2u_{12}u_{11}$, $u_2' = d_{48} - d_{49}$; $u_1' = d_{47} - d_{50} - d_{49}u_2'$, $u_0' = -d_{49}u_1' + d_{46} - d_{51} - d_{50}(d_{48} - d_{49})$; $$u' = x^3 + u_2'x^2 + u_1'x + u_0'$$	
2.2	compute the inverse α_1 of $t - s^2 - h$ modulo u'	16M+2SQ
	$g_1 = t_3 - h_3$, $g_0 = g_1(1 + u_2' + u_1' + u_0')$, $g_2 = t_0 - (d_5 + h_0 + g_1 u_0')$; $g_3 = t_3 + t_2 + t_1 + t_0 - (h_3 + h_2 + h_1 + h_0 + d_4 + d_6 + d_5 + g_0)$; $g_5 = (t_3 + t_2 + t_1 + t_0 - (h_3 + h_2 + h_1 + h_0 + d_4 + d_6 + d_5 + g_0) - (-t_3 + t_2 - t_1 + t_0 + h_3 - h_2 + h_1 - h_0 - d_4 + d_6 - d_5 - g_1(-1 + u_2' - u_1' + u_0')))/2$; $g_6 = g_3 - g_5 - g_2$, $g_7 = g_6 u_2' - g_5$, $g_8 = g_6^2$, $g_{10} = g_8 u_0' - g_7 g_2$; $g_{11} = g_8(1 + u_2' + u_1' + u_0') - (g_6 + g_7)(g_6 + g_5 + g_2) - g_{10}$, $g_{12} = g_{11}g_6$; $g_{13} = g_{11}g_5 - g_{10}g_6$, $g_9 = g_{11}^2$, $res_2 = g_9 g_2 - g_{13}g_{10}$, $\alpha_{10} = g_7 g_{13}$; $\alpha_{12} = g_6 g_{12}$, $\alpha_{11} = (g_6 + g_7)(g_{12} + g_{13}) - \alpha_{10} - \alpha_{12}$, $\alpha_{10} = \alpha_{10} + g_9$; $$\alpha_1 = \alpha_{12}x^2 + \alpha_{11}x + \alpha_{10}$$	
2.3	compute the remainder v of $\alpha_1(st - f_4)$ by u'	18M+I
	$i_1 = d_{10} - 1$, $i_2 = d_{13} - (d_{10} - 1)u_2'$, $i_3 = d_{11} - f_0 - i_2 u_0'$; $i_4 = d_{10} + d_{13} + d_{12} + d_{14} + d_{11} - (1 + f_2 + f_1 + f_0) - (i_2 + i_1)(u_2' + u_1' + u_0' + 1)$; $i_5 = (i_4 - ((d_{10} - d_{13} + d_{12} - d_{14} + d_{11} - 1 - f_2 + f_1 - f_0) - (i_2 - i_1)(u_2' - u_1' + u_0' - 1)))/2$; $i_6 = i_4 - i_3 - i_5$, $i_7 = (i_6 + i_5 + i_3)(\alpha_{12} + \alpha_{11} + \alpha_{10})$, $i_9 = i_6\alpha_{12}$, $i_{10} = i_3\alpha_{10}$; $i_8 = (i_6 - i_5 + i_3)(\alpha_{12} - \alpha_{11} + \alpha_{10})$, $i_{11} = (i_7 + i_8)/2 - (i_{10} + i_9)$; $i_{12} = (((4i_6 + 2i_5 + i_3)(4\alpha_{12} + 2\alpha_{11} + \alpha_{10}) - i_7 + i_8 - i_{10})/2 - 2(4i_9 + i_{11}))/3$; $i_{13} = i_7 - (i_{10} + i_{11} + i_{12} + i_9)$, $i_{14} = i_9$, $i_{15} = i_{12} - i_9 u_2'$, $i_{16} = i_{10} - i_{15}u_0'$; $i_{17} = (i_9 + i_{12} + i_{11} + i_{13} + i_{10}) - (i_{15} + i_{14})(u_2' + u_1' + u_0' + 1)$; $i_{18} = (i_{17} - (i_9 - i_{12} + i_{11} - i_{13} + i_{10}) + (i_{15} - i_{14})(u_2' - u_1' + u_0' - 1))/2$; $i_{19} = i_{17} - i_{16} - i_{18}$, $inv_2 = (res_2 \cdot i_{19})^{-1}$, $i_{20} = inv_2 \cdot i_{19}$; $v_0 = i_{20}i_{16}$, $v_1 = i_{20}i_{18}$, $v_2 = i_{20}i_{19}$; $$v = v_2 x^2 + v_1 x + v_0$$	

3	compute $u := u_{2D_1}$	16M+3SQ
	$j_1 = inv_2 \cdot res_2^2, j_2 = j_1^3, j_3 = j_1 v_1, j_4 = j_3^2, j_5 = j_1 v_0, j_6 = j_3(j_4 + 6j_5);$	
$*_4$	$j_7 = (v_2+v_1+v_0)(h_3+h_2+h_1), j_8 = (v_2-v_1+v_0)(h_3-h_2+h_1), j_9 = v_2 h_3;$	(8M)
	$j_{10} = v_0 h_1, j_{11} = (j_7+j_8)/2 - (j_{10}+j_9), j_{12} = 3j_3 + j_2 j_9, j_{14} = j_6 + j_2 j_{11};$	
	$j_{13} = 3(j_5+j_4) - j_2 + j_2((((4v_2+2v_1+v_0)(4h_3+2h_2+h_1) - j_7 + j_8 - j_{10})/2 - 2(4j_9+j_{11}))/3);$	
	$u_2 = j_{12} - u_2', u_1 = j_{13} - u_1' - u_2' u_2, u_0 = -u_2' u_1 + j_{14} - u_0' - u_1'(j_{12}-u_2');$ $u = x^3 + u_2 x^2 + u_1 x + u_0$	
total		165M, 20SQ, 2I

TABLE 3. If $h_3 = 0$ then replace $*_1, *_2, *_3$ and $*_4$ by

$*_1$	$inv_1 = c_{10}^{-1}, c_{14} = inv_1, c_{15} = inv_1 \cdot c_9, c_{16} = 1;$	(M+I)
$*_2$	$d_{27} = (t_3 + t_2 + t_1)(h_1 + h_2 + d_4 + d_6 - 2(t_3 + t_2 + t_1));$	(9M+SQ)
	$d_{28} = (t_3 - t_2 + t_1)(h_1 - h_2 + d_6 - d_4 - 2(t_3 - t_2 + t_1));$	
	$d_{29} = (4t_3 + 2t_2 + t_1)(-8t_3 + 2(d_4 - 2t_2 + h_2) + d_6 - 2t_1 + h_1);$	
	$d_{30} = -2t_3^2, d_{31} = t_1(d_6 - 2t_1 + h_1), d_{32} = (d_{27} + d_{28})/2 - (d_{31} + d_{30});$	
	$d_{33} = ((d_{29} - d_{27} + d_{28} - d_{31})/2 - 2(4d_{30} + d_{32}))/3;$	
	$d_{35} = (h_2 + h_1 + h_0)(d_{30} + d_{33} + d_{32} + s_0 + s_1);$	
	$d_{36} = (h_2 - h_1 + h_0)(d_{30} - d_{33} + d_{32} + s_0 - s_1);$	
	$d_{37} = (4h_2 + 2h_1 + h_0)(4d_{30} + 2(d_{33} + s_1) + d_{32} + s_0);$	
	$d_{43} = h_2 d_{30}, d_{39} = h_0(d_{32} + s_0), d_{41} = (d_{35} + d_{36})/2 - (d_{39} + d_{43});$	
	$d_{42} = ((d_{37} - d_{35} + d_{36} - d_{39})/2 - 2(4d_{43} + d_{41}))/3;$	
	$d_{40} = d_{35} - (d_{39} + d_{41} + d_{42} + d_{43}), d_{44} = 0;$	
$*_3$		
$*_4$	$j_{11} = v_2 h_2, j_{12} = 3j_3, j_{13} = 3(j_5 + j_4) - j_2 + j_2 j_{11};$	(5M)
	$j_{14} = j_6 + j_2((v_2 + v_1)(h_2 + h_1) - (v_1 h_1 + j_{11}));$	

TABLE 4. If $h_3, h_2 = 0$ then replace $*_1, *_2, *_3$ and $*_4$ by

$*_1$	$inv_1 = c_{10}^{-1}, c_{14} = inv_1, c_{15} = inv_1 \cdot c_9, c_{16} = 1;$	(M+I)
$*_2$	$d_{37} = -2t_3^2, d_{35} = t_2(d_4 - 2t_2), d_{38} = 0, d_{39} = 0, d_{43} = 0, d_{44} = 0;$	(5M+SQ)
	$d_{36} = (t_3 + t_2)(d_4 - 2(t_3 + t_2)) - (d_{35} + d_{37}), d_{42} = h_1 d_{37}, d_{40} = h_0(d_{36} + s_1);$	
	$d_{41} = (h_1 + h_0)(d_{37} + d_{36} + s_1) - (d_{40} + d_{42});$	
$*_3$		
$*_4$	$j_{12} = 3j_3, j_{13} = 3(j_5 + j_4) - j_2, j_{14} = j_6 + j_2(h_1 v_2);$	(2M)

TABLE 5. If $h_3, h_2, h_1 = 0$ then replace $*_1, *_2, *_3$ and $*_4$ by

$*_1$	$inv_1 = c_{10}^{-1}, c_{14} = inv_1, c_{15} = inv_1 \cdot c_9, c_{16} = 1;$	(M+I)
$*_2$	$d_{41} = -2h_0 t_3^2, d_{38} = 0, d_{39} = 0, d_{40} = 0, d_{42} = 0, d_{43} = 0, d_{44} = 0;$	(M+SQ)
$*_3$		
$*_4$	$j_{12} = 3j_3, j_{13} = 3(j_5 + j_4) - j_2, j_{14} = j_6;$	

TABLE 6. If $h_3, h_2, h_1, h_0 = 0$ then replace $*_1, *_2, *_3$ and $*_4$ by

$*_1$	$inv_1 = c_{10}^{-1}, c_{14} = inv_1, c_{15} = inv_1 \cdot c_9, c_{16} = 1;$	(M+I)
$*_2$	$d_{38} = 0, d_{39} = 0, d_{40} = 0, d_{41} = 0, d_{42} = 0, d_{43} = 0, d_{44} = 0;$	
$*_3$		
$*_4$	$j_{12} = 3j_3, j_{13} = 3(j_5 + j_4) - j_2, j_{14} = j_6;$	

References

[1] S. Abhyankar. Remark on Hessians and flexes. *Nieuw Arch. Wisk.*, 11:110–117, 1963.

[2] R. M. Avanzi, G. Frey, T. Lange, and R. Oyono. On using expansions to the base of -2. *Inter. J. of. Comp. Math.*, 81(4):403–406, 2004.

[3] E. Reinaldo Barreiro, J. Estrada Sarlabous, and J. P. Cherdieu. Efficient reduction on the Jacobian variety of Picard curves. In *Coding theory, cryptography and related areas (Guanajuato, 1998)*, pages 13–28. Springer, Berlin, 2000.

[4] A. Basiri, A. Enge, J-C. Faugère, and N. Gürel. Implementing the Arithmetic of $C_{3,4}$ Curves. In *Algorithmic Number Theory Symposium - ANTS-VI*, volume 3076 of *LNCS*, pages 87–101. Springer, 2004.

[5] R. Blache, J. Estrada Sarlabous, and M. Petkova. A geometric interpretation of reduction in the Jacobian of C_{ab} curves. preprint.

[6] C. Diem and E. Thomé. Index calculus in class groups of non-hyperelliptic curves of genus three. accepted at J. of Cryptology, 2007.

[7] K. E. Lauter E. W. Howe and J. Top. Pointless curves of genus three and four. In *Algebra, Geometry, and Coding Theory (AGCT 2003) (Y. Aubry and G. Lachaud, eds.)*, volume 11 of *Séminaires et Congrès*. Société Mathématique de France, Paris, 2005.

[8] S. Flon and R. Oyono. Fast arithmetic on Jacobians of Picard curves. In *Public Key Cryptography - PKC 2004*, volume 2947 of *LNCS*, pages 55–68. Springer, 2004.

[9] S. Flon, R. Oyono, and C. Ritzenthaler. Rationality of the intersection points of a line with a plane quartic. in progress, 2007.

[10] G. Frey and M. Müller. Arithmetic of modular curves and applications. In *Algorithmic Algebra and Number Theory*, pages 11–48. Ed. Matzat et al., Springer-Verlag, Berlin, 1999.

[11] S. D. Galbraith. *Equations for modular curves*. PhD thesis, Oxford, 1996.

[12] M. Gonda, K. Matsuo, K. Aoki, J. Chao, and S. Tsujii. Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementations. In *SCIS 2004*, 2004.

[13] E. González-Jiménez and R. Oyono. Non-hyperelliptic modular curves of genus 3. preprint, 2007.

[14] R. Harasawa and J. Suzuki. Fast Jacobian group arithmetic on C_{ab} curves. 1838:359–376, 2000.

[15] M. Homma. Funny plane curves in characteristic $p > 0$. *Comm. Algebra*, 15:1469–1501, 1987.

[16] K. Khuri-Makdisi. Linear algebra algorithms for divisor on an algebraic curve. *Math. of Computations*, 73:333–357, 2004.

[17] K. Khuri-Makdisi. asymptotically fast group operations on Jacobian of general curves. 2006. Available on `http://arxiv.org/abs/math.NT/0409209`.

[18] K. Miura and H. Yoshihara. Field theory for function fields of plane quartic curves. *J. of Algebra*, 226:283–294, 2000.

[19] E. Nart and C. Ritzenthaler. Non hyperelliptic curves of genus three over finite fields of characteristic two. *J. of Number Theory*, 116:443–473, 2006.

[20] G. Orzech and M. Orzech. *Plane algebraic curves*, volume 61. Pure and Applied Math., New-York, 1981.

[21] C. Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In *Algorithmic Number Theory Symposium - ANTS-VI*, volume 3076 of *LNCS*, pages 379–394. Springer, 2004.

[22] F. Abu Salem and K. Khuri-Makdisi. Fast Jacobian group operations for $C_{3,4}$ curves over a large finite field. Available at `http://www-lb.cs.aub.edu.lb/fa21/articleOct3.pdf`.

[23] J. Estrada Sarlabous, E. Reinaldo Barreiro, and J. A. Piñeiro Barceló. On the Jacobian varieties of Picard curves: explicit addition law and algebraic structure. *Math. Nachr.*, 208:149–166, 1999.

[24] Karl-Otto Stöhr and José Felipe Voloch. Weierstrass points and curves over finite fields. *Proc. Lond. Math. Soc., III. Ser.*, 52:1–19, 1986.

[25] F. Torres. The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs. Available on `http://arxiv.org/abs/math.AG/0011091`, 2000.

[26] A.M. Vermeulen. *Weierstrass points of weight two on curves of genus* 3. PhD thesis, Universiteit van Amsterdam, 1983.

UFR DE MATHÉMATIQUES, CITÉ SCIENTIFIQUE, F-59655 VILLENEUVE D'ASCQ, FRANCE
E-mail address: `Stephane.Flon@math.univ-lille1.fr`

DEPARTMENT OF COMBINATORICS AND OPTIMIZATIONS, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, N2L 3G1, CANADA
E-mail address: `royono@math.uwaterloo.ca`

INSTITUT DE MATHÉMATIQUES DE LUMINY, UMR 6206 DU CNRS, LUMINY, CASE 907, 13288 MARSEILLE, FRANCE.
E-mail address: `ritzenth@iml.univ-mrs.fr`