Fast Arithmetic on Jacobians of Picard Curves

Stéphane Flon[1] and Roger Oyono[2] *

[1] Mathematisches Institut, Universität Bonn, Beringstr. 4, 53115 Bonn, Germany
flon@math.uni-bonn.de
[2] IEM, Universität Essen, Ellernstr. 29, 45326 Essen, Germany
oyono@exp-math.uni-essen.de

Abstract. In this paper we present a fast addition algorithm in the Jacobian of a Picard curve over a finite field $\mathbb{F}_q$ of characteristic different from 3. This algorithm has a nice geometric interpretation, comparable to the classic "chord and tangent" law for the elliptic curves. Computational cost for addition is $144M+12SQ+2I$ and $158M+16SQ+2I$ for doubling.

Introduction

The discrete logarithm problem (DLP) is one of the two main problems on which public key cryptography is based (the other one being integer factorisation, in RSA cryptosystem): for example, Diffie-Hellman key exchange protocol [3] and ElGamal cryptosystem [4] are based on this problem.

In 1987, Miller [16] and Koblitz [11] suggested (independently) the use of the group of points of an elliptic curve over a finite field for DLP. It is now a well treated subject, and is even used in some industrial applications. Most of today's research is focused on the natural generalization of this example: DLP in the Jacobian of higher genus curves. One advantage is that, given an abstract finite group, one can use smaller fields (as Hasse-Weil formula shows).

In order to produce cryptosystems based on these Jacobian varieties, the first thing to worry about is to have secure cryptosystems (see [12] to find secure Picard curves). Still, it is very important to compute efficiently in the group, and an important part of today's reseach is devoted to allow fast arithmetic in Jacobians of curves. For instance, many papers study the case of hyperelliptic curves of genus 2 and 3 ([14, 15, 13, 19]).

In this article, we find explicit formulae for computing in the Jacobian of a Picard curve, basing us on some geometric aspects of these curves. Volcheck [23], Huang and Ierardi [10] already proposed general methods for computing in the Jacobians of arbitrary algebraic curves. These algorithms are not practical from a computational point of view though, and in addition they need to extend the base field. Hess' paper [9] is closer to our geometrical point of view, in such as it provides an explicit version of Riemann-Roch theorem (see also [8]).

* This work was supported by the European Community's Human Potential Programme (G.T.E.M. network) for the first author and by DFG for the second one.

1 Preliminaries and notations

1.1 Jacobian varieties of algebraic curves

In this section, we briefly recall fundamental facts on Picard groups and Jacobians. The letter k stands for an arbitrary perfect field, and $\overline{k}$ denotes a given algebraic closure of k.

Let C be a complete non-singular curve over k. The *divisor group of* C is the free abelian group $\mathrm{Div}(C)$ consisting of formal sums $\sum_{P\in C(\overline{k})} m_P \cdot P$, in which the m_P's are integers, finitely many of them being non-zero. Each divisor consists in an obvious way of a *positive part* and a *negative part*. It is called *effective* if there is no negative part.

A divisor is *defined over* k if it is fixed by the natural Galois action of $\mathrm{Gal}\,(\overline{k}|k)$. The *divisor group of* C *over* k, denoted $\mathrm{Div}_k(C)$, is the group of elements of $\mathrm{Div}(C)$ defined over k.

Given any $D = \sum_{P\in C(\overline{k})} m_P \cdot P \in \mathrm{Div}(C)$, one can define the *degree of* D, denoted $deg(D)$, as $\sum_P m_P$.

Let f be a non-zero element of the function field of C. Then, the *divisor* of f is

$$(f) := \sum_{P\in C(\overline{k})} v_P(f)\cdot P$$

where $v_P(f)$ denotes the valuation of f in the discrete valuation ring $\overline{k}[C]_P$.

Any such divisor is called a *principal divisor*, and two divisors are said to be *equivalent* if they differ from a principal divisor. One can check that any principal divisor is indeed a degree zero divisor. Moreover, if f is defined over k, then $(f) \in \mathrm{Div}_k(C)$.

The *divisor class group (or the Picard group)*, denoted $\mathrm{Pic}(C)$, is then the quotient of the group $\mathrm{Div}(C)$ by the subgroup of principal divisors. We let $\mathrm{Pic}_k(C)$ be the subgroup of $\mathrm{Pic}(C)$ fixed by the natural Galois action of $\mathrm{Gal}\,(\overline{k}|k)$. If we substitute $\mathrm{Div}(C)$ by $\mathrm{Div}^0(C)$, we respectively obtain the *degree* 0 *part of the divisor class group of* C, denoted $\mathrm{Pic}^0(C)$, and its subgroup $\mathrm{Pic}^0_k(C)$.

The most important and striking fact about $\mathrm{Pic}^0_k(C)$ is that it admits a kind of a "reification" (as D. Mumford suggestively presents them), the *Jacobian variety* J_C of C. More precisely, J_C represents a functor attached to the Picard group of C (see [17] for a very dense introduction to Jacobian varieties). It is automatically an abelian variety, whose dimension is the genus of C. Moreover, for each field L such that C has a L-rational point, the group $J_C(L)$ is canonically isomorphic to $\mathrm{Pic}^0_L(C)$.

Suppose the curve C has an affine model over k, with only one point at infinity (this is the case for Picard curves). Then, one can see the Jacobian in a third way, namely as the *ideal class group* of the integral closure of $k[x]$ in $k(C)$ (which is a Dedekind ring) associated to this model ([5, p. 6] or [7]). The sum of two divisors corresponds to the product of the associated ideals.

Of course, it may appear obvious to compute in the Jacobian (or, equivalently, in the degree zero Picard group): the sum of two divisors is just the resulting formal sum. But it is of considerable importance for cryptographic ends to have a unique and concise way to express divisors. This leads to the notion of a *reduced divisor*. Indeed, a consequence of Riemann-Roch theorem is the following representation theorem of divisors:

Theorem 1 (Representation by reduced divisors). *Let C be a non-singular curve over k of genus g, with a given k-point P_∞. Let D be an element of $Div_k^0(C)$. Then, there exists an effective divisor E over k of degree $m \leq g$, whose support does not contain P_∞, and such that $E - m \cdot P_\infty$ is equivalent to D (we refer to such a divisor as an* almost reduced divisor*).*

It is unique if we demand m to be minimal, and it is then called the reduced representation *of (the divisor class of) D.*

1.2 Picard curves and their Jacobians

In the following k is any field of characteristic different from 3.

A *Picard curve* is a genus 3 cyclic trigonal curve. Any Picard curve C admits a projective model of the following form

$$z \cdot y^3 = z^4 \cdot f_4(x/z)$$

where f_4 is a monic degree 4 separable polynomial of one variable over k. It has a unique point at infinity, P_∞, namely $(0 : 1 : 0)$.

Any Picard curve C appears as a cyclic Galois cover of degree 3 of the projective line, with 5 (totally) ramified points (including P_∞). The automorphism group of this cover is generated by

$$\sigma : (x : y : z) \mapsto (x : \zeta y : z)$$

where ζ is a non-trivial cubic root of unity. Two points are *conjugate* if they lie on the same geometric fibre of the cover. Each non-ramification point P of C has thus two *conjugate points*, namely P^σ and P^{σ^2}.

Note that $v_{P_\infty}(x) = -3$ and $v_{P_\infty}(y) = -4$. Let f be a polynomial in $k[x, y]$, of degree m, not lying in the ideal of C. According to Bézout theorem (as C is irreducible), the intersection multiplicity of f with C at P_∞, denoted by $\mathrm{ord}_\infty(f)$, is equal to $4m + v_{P_\infty}(f)$.

In the following, we will use the so-called "Mumford representation" of divisors. This represention arises from the one proposed in [18], page 3.17, for reduced divisors of hyperelliptic curves. One may see it as an interpolation theorem for the points in the support of the divisor. This is harmless for hyperelliptic curves, as there can not be any pair of conjugate points in the support of a reduced divisor of a hyperelliptic curve. Unfortunately, this is not true anymore for Picard curves, and in fact Mumford representation is only suitable for a peculiar (but very likely) class of reduced divisors, namely the ones that do not have any two conjugate points in their support (they are called *typical* in [2], a terminology that we will keep in this paper).

Theorem 2 (Reduced divisors and Mumford representation). *An almost reduced divisor is not reduced if and only if its positive part D_0 is of degree 3, and such that there exists a line l with $(l)_0 \geq D_0$.*

Let D be a typical reduced divisor over k. It can then be uniquely represented as the intersection divisor of u and $y - v$, with:

- $u, v \in k[x]$,
- u *monic,*
- $\deg(v) < \deg(u) \leq 3$, *and*
- $u | v^3 - f_4$.

Note 1. For any typical reduced divisor D, we will note its Mumford representation polynomials by u_D and $y - v_D$. In the ideal class group, D corresponds to $< u_D, y - v_D >$.

Proof. The presented proof differs from the one of [2].

First of all, let us treat the case where $D_0 = P + Q$ is of degree 2. Suppose we have $P + Q - 2 \cdot P_\infty = R - P_\infty + (f)$ for a $f \in k(C)$. Then,

$$P + Q + R^\sigma + R^{\sigma^2} - 4 \cdot P_\infty = (f_1)$$

for a $f_1 \in k(C)$. As $v_{P_\infty}(f_1) = -4$, f_1 must be a line not passing through P_∞. This contradicts the fact that it goes through R^σ and R^{σ^2}.

Suppose now that $D = P_1 + P_2 + P_3 - 3 \cdot P_\infty$. The divisor D can not be equivalent to some $R - P_\infty$, because this would prove the existence of a polynomial f such that $v_{P_\infty}(f) = -5$.

If D is equivalent to some $Q_1 + Q_2 - 2 \cdot P_\infty$, we have to distinguish two cases, namely whether Q_1 and Q_2 are conjugate or not.

If they are not conjugate, then

$$P_1 + P_2 + P_3 + Q_1^\sigma + Q_1^{\sigma^2} + Q_2^\sigma + Q_2^{\sigma^2} - 7 \cdot P_\infty = (f)$$

with f a conic crossing C once through P_∞. It crosses the line $(Q_1 P_\infty)$ (resp. $(Q_2 P_\infty)$) in three points, thus it should contain these two lines. This contradicts the previous statement.

In the remaining case (D equivalent to $Q_1 + Q_1^\sigma - 2 \cdot P_\infty$), one has

$$P_1 + P_2 + P_3 + Q_1^{\sigma^2} - 4 \cdot P_\infty = (f)$$

This means that there exists a line f such that $(f)_0 \geq P_1 + P_2 + P_3$.

The second part of the theorem is straightforward. □

Remark 1. In the case of a non-typical divisor $D = P_1 + P_1^\sigma + P_2$, then one can write D as the intersection divisor of $u \in k[x]$ (corresponding to the two lines $(P_1 P_\infty)$ and $(P_2 P_\infty)$), $\deg(u) \leq 2$, with an element of the k-vector space spanned by $1, x, y, x^2, y^2, xy$ (corresponding to the two lines $(P_1 P_2)$ and $(P_1^\sigma P_2)$).

The presented algorithm in the next section only works for typical divisors, and the result is an almost reduced divisor, which is with very high probability a typical one.

2 Fast addition algorithm for Jacobian of Picard curves

2.1 Main algorithm

As said in the introduction, the following algorithm is inspired by the "chord and tangent" law on the group of points of an elliptic curve. In our case, we will have to replace the chord or the tangent by a cubic, and we will introduce a conic in order to get the opposite of a divisor. Note that for an elliptic curve, or even a hyperelliptic curve, the latter operation requires no computation.

In [20], the authors make use of similar geometric constructions to propose a reduction algorithm. Instead of using a cubic, they work recursively, reducing a degree 4 effective divisor into a degree ≤ 3 effective divisor, with the help of two conics. Their algorithm requires to work with rational points (or to perform some field extensions). It also requires to make a final factorisation of a polynomial in $k[x]$ of degree at most 3. As our algorithm is completely explicit (i.e. we only perform some elementary operations in the base field k), we will not need any of these requirements.

Geometric description of the Jacobian group addition. In the most common case, we have two typical reduced divisors $D_1 := P_1 + P_2 + P_3 - 3 \cdot P_\infty$ and $D_2 := Q_1 + Q_2 + Q_3 - 3 \cdot P_\infty$, and we want to find the reduced divisor equivalent to $P_1 + P_2 + P_3 + Q_1 + Q_2 + Q_3 - 6 \cdot P_\infty$. Let us consider the divisor

$$D := -(P_1 + P_2 + P_3 + Q_1 + Q_2 + Q_3 - 9 \cdot P_\infty)$$

This is a degree 3 divisor defined over k. Riemann-Roch theorem asserts that

$$l(D) - l(K - D) = \deg(D) + 1 - g = 1$$

(where K stands for the canonical divisor), so that in any case $l(D) \geq 1$.

In particular, there exists a w in $k(C)$ such that $(w) \geq -D$. As the only pole of w is P_∞, it is a polynomial in $k[x, y]$. Moreover, as $v_{P_\infty}(w) \geq -9$, one knows that w is an element of the k-vector space spanned by $1, x, x^2, xy, y, y^2, x^3$. From now on, we take w to be the unique such element (up to a multiplicative factor) with maximal valuation at P_∞.

If w is a conic, a very unlikely situation, then geometric considerations on $J(C)$ allow a very easy computation of the reduction of $D_1 + D_2$. Let us illustrate this in the case where the support of $D_1 + D_2$ consists of six points aside from P_∞ that lie on a (unique) conic, not going through P_∞. Then the conic crosses C in exactly two more points Q_1 and Q_2. Taking the line through those two points gives us two new points K_1 and K_2, such that $K_1 + K_2 - 2 \cdot P_\infty$ is the reduction of $D_1 + D_2$ (see Fig. 1).

If w is a cubic, Bézout theorem asserts that the corresponding variety crosses C in exactly three more points, say R_1, R_2 and R_3. One has the obvious relation

$$(P_1+P_2+P_3-3\cdot P_\infty)+(Q_1+Q_2+Q_3-3\cdot P_\infty) = -(R_1+R_2+R_3-3\cdot P_\infty)+(w)$$

Fig. 1. Case where w is a conic

so that we have obtained an almost reduced form of the opposite of $D_1 + D_2$.

Using Riemann-Roch in the same way as we have just done, one can show that there exists a unique conic v going through R_1, R_2, R_3 and twice in P_∞. It crosses C in three further points K_1, K_2, K_3, and by construction, $K_1+K_2+K_3-3\cdot P_\infty$ is in the class of $D_1 + D_2$.

One can roughly sum-up how the algorithm works by Fig. 2.

Algebraic interpretation and formulae. The presented algorithm can be naturally divided into three steps: finding w, reduce $-(D_1 + D_2)$, and then taking the opposite (with the conic). Now we give an algebraic interpretation of these steps.

First step: computation of the cubic

This is the only step where one has to distinguish between addition and doubling.

Addition

First of all, let us treat the most common case, in which w can be expressed as

$$w = y^2 + s \cdot y + t$$

where s and t are polynomials in x, with $\deg(s) \leq 1$ and $\deg(t) \leq 3$. As the support of D_1 (resp. D_2) is contained in the support of (w), we are naturally led to find three polynomials s, δ_1 and δ_2 in x, of degree ≤ 1, such that

$$w = (y - v_1) \cdot (y + v_1 + s) + u_1 \cdot \delta_1 = (y - v_2) \cdot (y + v_2 + s) + u_2 \cdot \delta_2$$

It is easy to see that the leading coefficient of δ_1 (resp. δ_2) has to be the square of that of v_1 (resp. v_2).

Fig. 2. Description of the algorithm

It then leads to the unique condition:

$$(v_1 + v_2 + s) \cdot (v_1 - v_2) + u_2 \cdot \delta_2 - u_1 \cdot \delta_1 = 0$$

In case w has no y^2 term, then the same strategy gives the condition

$$s \cdot (v_1 - v_2) + \delta_2 \cdot u_2 - \delta_1 \cdot u_1 = 0$$

where δ_1 and δ_2 are constant polynomials.

Note that these two equations are very similar. In fact, during the computation of s and δ_1, we consider in both subcases the remainder r of $t_1 \cdot u_1$ by u_2, where t_1 is the inverse of $v_1 - v_2$ modulo u_2. It turns out that if r is of degree 2, then we are in the first subcase, if not we are in the second one.

The only remaining case is a trivial one; namely when the points of the support of D_1 are conjugate of the points of the support of D_2.

Doubling

In that case, we are looking for a w in the ideal $I^2 =< u_1^2, u_1 \cdot (y - v_1), (y - v_1)^2 >$. Here we only treat the main subcase, where w has a y^2 part, and hence when w can be written in the following manner:

$$(y - v_1) \cdot (y + v_1 + s) + u_1 \cdot \delta_1$$

(the other subcases are either similar or trivial, and very unlikely anyway). The unique condition, obtained in the same way as above, is then

$$(y - v_1) \cdot (2v_1 + s) + u_1 \cdot \delta_1 \in I^2$$

In other respects, an easy computation shows that:

$$3v_1^2\,(y - v_1) - u_1 \cdot w_1 \in I^2$$

where w_1 is defined by $v_1^3 - f_4 = u_1 \cdot w_1$.

This implies that

$$3v_1^2 u_1 \cdot \delta_1 + (2v_1 + s) \cdot u_1 \cdot w_1 \in I^2$$

If v_1 is prime to u_1, that is if the support of D_1 does not contain any ramification point (different from P_∞), then we have

$$u_1 |\left(3v_1^2 \cdot \delta_1 + (2v_1 + s) \cdot w_1\right)$$

and the computation of the inverse of w_1 in $k[x]/(u_1)$ gives us δ_1, and then s.

Remark 2. If the support of $D_1 + 3 \cdot P_\infty$ does contain a ramification point, then the geometry of the curve allows us to compute the reduction of $2 \cdot D_1$ easily.

Second step: computation of $-(D_1 + D_2)$

Here, we only treat the most common case (which is also the most difficult one), namely when w has a y^2 term, and hence can be written

$$w = y^2 + s \cdot y + t^3$$

with $s, t \in k[x]$, $\deg(s) \leq 1$ and $\deg(t) \leq 3$.

We already know how to characterize the reduced divisor equivalent to $-(D_1 + D_2)$: it suffices to compute the intersection divisor of the (variety attached to the) cubic w with C.

A way to find $u_{-(D_1+D_2)}$ is thus to compute the resultant $\mathrm{Res}(w, C)$ of w with $y^3 - f_4$ (relative to y), to compute the quotient of $\mathrm{Res}(w, C)$ by $u_1 \cdot u_2$, and then to normalize.

To compute $v_{-(D_1+D_2)}$, one can exploit the relation

$$(t - s^2) \cdot v_{-(D_1+D_2)} \equiv (s \cdot t - f_4) \mathrm{mod}(u_{-(D_1+D_2)})$$

so that $v_{-(D_1+D_2)}$ is the remainder of the quotient of $\alpha_1 \cdot (s \cdot t - f_4)$ by $u_{-(D_1+D_2)}$, where α_1 is the inverse of $t - s^2$ in $k[x, y]/(u_{-(D_1+D_2)})$.

Third step: computation of $D_1 + D_2$

Obviously, one has $v_{D_1+D_2} = v_{-(D_1+D_2)}$. Thus, we are reduced to compute $u_{D_1+D_2}$. It is easily obtained as the (normalized) euclidean quotient of $(v_{D_1+D_2})^3 - f_4$ by $u_{-(D_1+D_2)}$.

2.2 Explicit formulae in the most common case

The given algorithms correspond to the case when w has a y^2 term. Note that in order to speed up the algorithm, we have used Karatsuba tricks to multiply two polynomials. Similarly, we only compute the coefficients we need in the algorithm. For instance, as we only need to know the quotient of the resultant of w and C by $u_1 \cdot u_2$, the degree ≤ 5 part of this resultant is irrelevant. The reader can find the tables for addition and doubling at the end in the appendix of this article.

3 Remarks and outlook

As far as we know, the presented algorithm for computing in the Jacobian of a Picard curve is quite efficient. In [2, p. 24], the authors present estimations for the cost of various algorithms computing the reduction of a typical divisor of degree 6 in the Jacobian of a Picard curve. The most efficient algorithm is supposed to need roughly $150M$ and $6I$. The composition in itself has a computational cost of about $50M$ and $1I$.

The cost for addition in the Jacobian of hyperelliptic curves of genus 3 is substantially lower than ours (it is about $I + 70M + 6SQ$, see [19]). On the other hand, for cryptographic purposes, scalar multiplication is the main topic. In that respect, our algorithm benefits from the two following remarks, which should approximately halve the complexity: one can speed up scalar multiplication using the fast automorphism σ defined p. 3, (see [6]), and rather use -2-adic expansions instead of 2-adic usual expansions (see [1]).

Our viewpoint was definitely geometric, and we did not separate composition from reduction. One may hope that this viewpoint can be generalised to a much broader class of curves. This statement is strenghtened by the fact that Cantor algorithm and its improvements [14] for computing in the Jacobian of a hyperelliptic curve of genus 2 can be interpreted in the very same way as our algorithm. Note though that this case is the only one where Cantor's algorithm and ours coincide.

We have presented formulae for Picard curves. We stress the fact that they are immediately adaptable to non-singular curves of genus 3 with a hyperflex. In that case, addition requires $160M + 17SQ + 2I$ and a doubling requires $177M + 21SQ + 2I$.

Acknowledgements

The authors would like to thank Gerhard Frey for the valuable ideas he gave, as well Tanja Lange for reading the manuscript in depth, and also for the support she provided. We also thank the referees for their comments, and Roberto Avanzi for pointing out to us the use of fast endomorphisms.

References

1. R. M. Avanzi, G. Frey, T. Lange, and R. Oyono. On using expansions to the base of -2. submitted, see arXiv, math.NT/0312060,2003, 2003.
2. A. Basiri, A. Enge, J-C. Faugère, and N. Gürel. The arithmetic of Jacobian groups of superelliptic cubics. Technical report, INRIA, 2002.
3. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE transactions on information theory*, 22:644–654, 1976.
4. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31-4:469–472, 1985.
5. S. Galbraith, S.M. Paulus, and N. Smart. Arithmetic on superelliptic curves. *Math. Comp.*, 71(237):393–405, 2002.
6. R. P. Gallant, J. L. Lambert, and S. A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *Advances in Cryptology – Crypto'2001*, volume 2139 of *Lect. Notes Comput. Sci.*, pages 190–200. Springer, 2001.
7. R. Hartshorne. *Algebraic geometry*, volume 52. Springer-Verlag, GTM, 1977.
8. F. Hess. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern.* PhD thesis, TU Berlin, 1999.
9. F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comp.*, 33(4):425–445, 2002.
10. M-D. Huang and D. Ierardi. Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. *J. of symb. comp.*, 18:519–539, 1994.
11. N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.
12. K. Koike and A. Weng. Construction of cryptographically secure cm-picard curves, 2003. preprint.
13. J. Kuroki, M. Gonda, K. Matsuo, J. Chao, and S. Tsujii. Fast genus three hyperelliptic curve cryptosystems. In *SCIS 2002*, 2002.
14. T. Lange. Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae. In *Cryptology ePrint archive*, Report 2002/121, 2002. http://eprint.iacr.org/.
15. K. Matsuo, J. Chao, and S. Tsujii. Fast genus two hyperelliptic curve cryptosystems. Technical report, IEICE, 2001. ISEC2001-31.
16. V.S. Miller. The use of elliptic curves in cryptography. In *Advances in cryptology-CRYPTO '85*, volume 218 of *LNCS*, pages 417–426, Santa Barbara, California, 1986. Springer-Verlag.
17. J-S. Milne. Jacobian varieties. In Cornell G. and J.H. Silverman, editors, *Arithmetic Geometry*, pages 167–212. Springer, 1986.
18. D. Mumford. *Tata lectures on theta II*, volume 43 of *Progress in mathematics.* Birkhaüser, 1984.
19. J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar. Hyperelliptic curves cryptosystems: closing the performance gap to elliptic curves. In *Cryptology ePrint archive*, 2003. http://eprint.iacr.org/.
20. 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*, volume 877, pages 13–28. Springer, 1998.
21. J.H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer-Verlag, GTM, 1994.
22. H. Stichtenoth. *Algebraic function fields and codes.* Springer-Verlag, 1993.
23. E. Volcheck. Computing in the Jacobian of a plane algebraic curve. In Adleman, editor, *ANTS-I*, volume 877, pages 221–233. Springer-Verlag, 1994.

Table 1. Addition, $\deg u_1 = \deg u_2 = 3$

Input	$D_1 = [u_1, v_1]$ and $D_2 = [u_2, v_2]$ $u_i = x^3 + u_{i2}x^2 + u_{i1}x + u_{i0}, v_i = v_{i2}x^2 + v_{i1}x + v_{i0}$ $f = x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$
Output	$D = [u_{D_1+D_2}, v_{D_1+D_2}] = D_1 + D_2$ with $u_{D_1+D_2} = x^3 + d_1x^2 + d_2x + d_3$ $v_{D_1+D_2} = v_2'x^2 + v_1'x + v_0'$

Step	Expression	Operations
1	compute resultant res_1 of $(v_1 - v_2)$ and u_2, and $z_1 := res_1/(v_1 - v_2) \bmod u_2$ $t_1 = u_{21}(v_{22} - v_{12})$, $t_2 = u_{22}(v_{22} - v_{12})$, $t_3 = u_{20}(v_{22} - v_{12})$; $t_4 = u_{22}(v_{20} - v_{10})$, $t_5 = u_{21}(v_{21} - v_{11})$, $t_6 = (v_{22} - v_{12})(t_1 + v_{10} - v_{20})$; $t_7 = (v_{21} - v_{11})(v_{21} - v_{11} - t_2)$, $t_8 = (t_4 - t_3 - t_5)(t_2 + v_{11} - v_{21})$; $t_9 = (v_{22} - v_{12})(t_4 - t_3 - t_5)$, $t_{10} = (v_{21} - v_{11})(v_{20} - v_{10} - t_1)$; $inv_0 = t_6 + t_7$, $t_{11} = inv_0 \cdot u_{22}$, $t_{12} = u_{20}(v_{21} - v_{11})$; $t_{13} = inv_0 \cdot t_{12}$, $t_{14} = t_3(t_9 - t_{10})$, $s_1 = (v_{20} - v_{10} - t_1)^2$; $inv_2 = t_8 + s_1$, $t_{15} = inv_2(v_{20} - v_{10})$; $inv_1 = t_{11} + t_9 - t_{10}$, $res_1 = t_{15} - t_{13} - t_{14}$; $z_1 = inv_0x^2 + inv_1x + inv_2$	15M+1SQ
2	compute the cubic $w = y^2 + sy + t$ $t_{16} = (u_{12} - u_{22})inv_0$, $t_{17} = (u_{11} - u_{21})inv_1$; $t_{18} = (u_{10} - u_{20})inv_2$, $t_{19} = (u_{12} + u_{11} - u_{22} - u_{21})(inv_0 + inv_1)$; $t_{20} = (u_{12} + u_{10} - u_{22} - u_{20})(inv_0 + inv_2)$; $t_{21} = (u_{11} + u_{10} - u_{21} - u_{20})(inv_1 + inv_2)$; $t_{22} = u_{22} \cdot t_{16}$, $t_{23} = u_{21} \cdot t_{16}$, $t_{24} = u_{22}(t_{22} + t_{16} + t_{17} - t_{19})$; $t_{25} = (u_{21} + u_{20})(t_{19} - t_{22} - t_{17})$, $t_{26} = u_{20}(t_{22} + t_{16} + t_{17} - t_{19})$; $r_0 = t_{24} + t_{20} + t_{17} - t_{23} - t_{16} - t_{18}$; $r_1 = t_{21} + t_{23} - t_{17} - t_{18} - t_{25} - t_{26}$, $r_2 = t_{18} + t_{26}$, $s_2 = v_{12}^2$; $t_{27} = r_0 \cdot res_1$, $t_{28} = r_0 \cdot s_2$, $t_{29} = r_0 \cdot t_{28}$, $t_{30} = t_{28} \cdot res_1$; $t_{31} = -res_1 \cdot (v_{12} + v_{22})$, $t_{32} = r_1 \cdot s_2$, $t_{33} = u_{22} \cdot t_{28}$; $\gamma_1 = t_{31} + t_{33} - t_{32}$, $t_{34} = res_1 \cdot \gamma_1$, $t_{35} = -t_{27}(v_{11} + v_{21})$; $t_{36} = -t_{27}(v_{10} + v_{20})$, $t_{37} = r_1\gamma_1$, $t_{38} = r_2 \cdot t_{28}$, $t_{39} = r_2 \cdot \gamma_1$; $t_{40} = u_{21} \cdot t_{29}$, $t_{41} = u_{20} \cdot t_{29}$; $\lambda_1 = t_{35} + t_{40} - t_{37} - t_{38}$, $\mu_1 = t_{36} + t_{41} - t_{39}$; $t_{42} = -t_{27} \cdot v_{12}$, $t_{43} = -t_{27} \cdot v_{11}$; $t_{44} = -t_{27} \cdot v_{10}$, $t_{45} = (v_{12} + v_{11})(t_{42} + t_{43} - \lambda_1)$; $t_{46} = v_{11}(t_{43} - \lambda_1)$, $t_{47} = (v_{12} + v_{10})(t_{42} + t_{44} - \mu_1)$; $t_{48} = v_{10}(t_{44} - \mu_1)$, $t_{49} = (v_{11} + v_{10})(t_{43} + t_{44} - \lambda_1 - \mu_1)$; $t_{50} = t_{30}(u_{12} + u_{11})$, $t_{51} = u_{11} \cdot t_{30}$, $t_{52} = t_{34}(u_{12} + u_{10})$, $t_{53} = u_{10} \cdot t_{34}$; $t_{54} = (u_{11} + u_{10})(t_{30} + t_{34})$, $B_0 = t_{34} + t_{50} + t_{45} + t_{30} - t_{51} - t_{46}$; $B_1 = t_{52} + t_{30} + t_{51} + t_{47} + t_{46} - t_{53} - t_{48}$; $B_2 = t_{54} + t_{49} - t_{51} - t_{53} - t_{46} - t_{48}$; $B_3 = t_{53} + t_{48}$; $t_{55} = B_0 \cdot t_{27}$, $i_1 = (t_{55})^{-1}$, $t_{56} = i_1 \cdot B_0$; $t_{57} = i_1 \cdot t_{27}$, $t_{58} = t_{57} \cdot t_{27}$, $t_{59} = t_{57} \cdot B_1$; $t_{60} = t_{57} \cdot B_2$, $t_{61} = t_{57} \cdot B_3$, $t_{62} = t_{56} \cdot \lambda_1$, $t_{63} = t_{56} \cdot \mu_1$; $t_{64} = t_{56} \cdot B_0$, $t_{65} = t_{56} \cdot B_1$, $t_{66} = t_{56} \cdot B_2$, $t_{67} = t_{56} \cdot B_3$; $w = y^2 + (t_{62}x + t_{63})y + t_{64}x^3 + t_{65}x^2 + t_{66}x + t_{67}$	52M+1SQ+1I
3	compute $res(w, C, y)$ $s_3 = t_{59}^2$, $t_{68} = t_{59}(6t_{60} + s_3)$, $s_4 = t_{62}^2$, $s_5 = (t_{62} + t_{63})^2$; $s_6 = t_{63}^2$, $t_{69} = t_{62}t_{64}$, $t_{70} = t_{62}(s_4 - 3t_{65})$; $t_{71} = t_{63}t_{64}$, $t_{72} = -3f_3t_{69}$, $t_{73} = t_{62}(s_5 - 3t_{66} - s_4 - s_6)$; $t_{74} = t_{63}(s_4 - 3t_{65})$, $t_{75} = f_3t_{70}$, $t_{76} = -3f_2t_{69}$, $t_{77} = -3f_3t_{71}$; $s_7 = t_{58}^2$, $t_{78} = t_{58}s_7$, $t_{79} = t_{78}(1 - 3t_{69})$; $t_{80} = t_{78}(t_{70} + t_{72} + 2f_3 - 3t_{71})$; $t_{81} = t_{78}(t_{73} + t_{74} + t_{75} + t_{76} + t_{77} + 2f_2 + f_3^2)$;	14M+5SQ
4	compute $u_{-(D_1+D_2)}$ $t_{82} = u_{12}u_{22}$, $t_{83} = u_{12}u_{21}$, $t_{84} = u_{11}u_{22}$; $t_{85} = (u_{11} + u_{21} + u_{10} + u_{20} + t_{82} + t_{83} + t_{84})(1 + t_{79} + 3t_{59} - u_{12} - u_{22})$; $t_{86} = (u_{10} + u_{20} + t_{83} + t_{84})(t_{79} + 3t_{59} - u_{12} - u_{22})$; $c_1 = t_{79} + 3t_{59} - u_{12} - u_{22}$, $t_{87} = c_1(u_{12} + u_{22})$; $c_2 = t_{80} + 3t_{60} + 3s_3 - u_{11} - u_{21} - t_{82} - t_{87}$, $t_{88} = c_2(u_{12} + u_{22})$; $c_3 = u_{11} + u_{21} + t_{68} + t_{81} + t_{82} + t_{86} + 3t_{61} - t_{88} - t_{85}$; $u_{-(D_1+D_2)} = x^3 + c_1x^2 + c_2x + c_3$	7M

5	compute $res(t-s^2, u_{-(D_1+D_2)}, x)$ and precomputations for $v_{D_1+D_2}$ $t_{89}=c_3t_{64},\ t_{90}=c_1t_{64},\ t_{91}=c_2t_{64},\ t_{92}=c_2(t_{65}-s_4);$ $t_{93}=c_1(t_{66}+s_4+s_6-s_5),\ t_{94}=c_3(t_{66}+s_4+s_6-s_5);$ $t_{95}=c_2(t_{67}-s_6),\ t_{96}=c_3(t_{65}-s_4),\ t_{97}=c_1(t_{67}-s_6);$ $s_8=(t_{89}+s_6-t_{67})^2,\ s_9=(t_{91}+s_5-t_{66}-s_4-s_6)^2;$ $t_{98}=(t_{94}-t_{95})(t_{90}+s_4-t_{65});$ $t_{99}=(s_8-t_{98})(t_{89}+t_{92}+s_6-t_{67}-t_{93});$ $t_{100}=(t_{96}-t_{97})(t_{90}-t_{65}+s_4);$ $t_{101}=(t_{91}+s_5-t_{66}-s_4-s_6)(t_{89}+s_6-t_{67});$ $t_{102}=(t_{96}-t_{97})(t_{100}-2t_{101});$ $t_{103}=s_9(t_{94}-t_{95}),\ res_2=t_{99}+t_{102}+t_{103};$ $t_{104}=(t_{90}+s_4-t_{65})(t_{92}+t_{89}+s_6-t_{93}-t_{67});$ $j_0=t_{104}-s_9,\ t_{105}=c_1j_0,\ t_{106}=c_1(t_{100}-t_{101});$ $t_{107}=c_2j_0,\ t_{108}=c_3(t_{66}+s_4+s_6-s_5);$ $t_{109}=(t_{108}-t_{95})(t_{90}+s_4-t_{65}),\ j_1=t_{105}+t_{101}-t_{100};$ $j_2=t_{107}+t_{109}-t_{106}-s_8,\ t_{110}=t_{62}(t_{65}+t_{66});$ $t_{111}=t_{62}t_{66},\ t_{112}=t_{63}(t_{65}+t_{67}),\ t_{113}=t_{63}t_{67};$ $t_{114}=(t_{62}+t_{63})(t_{66}+t_{67}),\ t_{115}=c_1(1-t_{69});$ $t_{116}=c_1(t_{115}+t_{71}+t_{110}-f_3-t_{111}),\ t_{117}=c_2(1-t_{69});$ $t_{118}=(c_2+c_3)(1+f_3+t_{111}-t_{69}-t_{115}-t_{71}-t_{110});$ $t_{119}=c_3(t_{115}+t_{71}+t_{110}-f_3-t_{111});$ $t_{120}=j_0(t_{116}+f_2+t_{113}-t_{117}-t_{112}-t_{111});$ $t_{121}=(j_0+j_1)(t_{116}+f_2+f_1+2t_{113}-t_{112}-t_{114}-t_{118}-t_{119});$ $t_{122}=j_1(f_1+t_{111}+t_{113}+t_{117}-t_{114}-t_{118}-t_{119});$ $t_{123}=(j_0+j_2)(t_{116}+f_2+f_0+t_{119}-t_{112}-t_{117}-t_{111});$ $t_{124}=j_2(f_0+t_{119}-t_{113});$ $t_{125}=(j_1+j_2)(f_1+f_0+t_{111}+t_{117}+t_{119}-t_{114}-t_{118}-t_{119});$ $t_{126}=c_1t_{120},\ t_{127}=c_2t_{120};$ $t_{128}=c_1(t_{126}+t_{120}+t_{122}-t_{121}),\ t_{129}=(c_2+c_3)(t_{121}-t_{126}-t_{122});$ $t_{130}=c_3(t_{126}+t_{120}+t_{122}-t_{121});$	42M+2SQ
6	compute $v_{D_1+D_2}$ $t_{131}=res_2(t_{128}+t_{123}+t_{122}-t_{127}-t_{120}-t_{124}),\ i_2=(t_{131})^{-1};$ $t_{132}=i_2(t_{128}+t_{123}+t_{122}-t_{127}-t_{120}-t_{124});$ $t_{133}=t_{132}(t_{128}+t_{123}+t_{122}-t_{127}-t_{120}-t_{124});$ $t_{134}=t_{132}(t_{125}+t_{127}-t_{122}-t_{124}-t_{129}-t_{130});$ $t_{135}=t_{132}(t_{124}+t_{130});$ $v'_2=-t_{133},\ v'_1=-t_{134},\ v'_0=-t_{135};$	5M+1I
7	compute $u_{D_1+D_2}$ $s_{10}=res_2^2,\ t_{136}=i_2s_{10},\ s_{11}=t_{136}^2,\ t_{137}=t_{136}s_{11};$ $t_{138}=t_{136}t_{134},\ s_{12}=t_{138}^2,\ t_{139}=t_{136}t_{135};$ $t_{140}=t_{138}(s_{12}+6t_{139}),\ t_{141}=t_{137}f_3;$ $t_{142}=c_1(3t_{138}-c_1),\ d_1=3t_{138}-c_1;$ $d_2=3t_{139}+3s_{12}+t_{137}-c_2-t_{142};$ $t_{143}=c_1d_2,\ t_{144}=c_2(3t_{138}-c_1);$ $d_3=t_{140}+t_{141}-c_3-t_{143}-t_{144};$	9M+3SQ
total		144M, 12S, 2I

Table 2. Doubling, $\deg u_1 = 3$

Input	$D_1 = [u_1, v_1]$ $u_1 = x^3 + u_{12}x^2 + u_{11}x + u_{10}, v_1 = v_{12}x^2 + v_{11}x + v_{10}$ $f = x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$
Output	$D = [u_{2D_1}, v_{2D_1}] = 2D_1$ with $u_{2D_1} = x^3 + d_1x^2 + d_2x + d_3$ $v_{2D_1} = v_2'x^2 + v_1'x + v_0'$

Step	Expression	Operations
1	compute w_1 such that $u_1w_1 = v_1^3 - f$ $s_1 = v_{12}^2$, $s_2 = v_{11}^2$, $t_1 = -s_1v_{12}$, $t_2 = -3s_1v_{11}$; $t_3 = v_{12}v_{10}$, $t_4 = -3v_{12}(t_3 + s_2)$; $t_5 = -v_{11}(s_2 + 6t_3)$, $t_6 = t_1u_{12}$, $t_7 = t_1u_{11}$; $t_8 = u_{12}(t_2 - t_6)$, $t_9 = u_{12}(t_4 + 1 - t_7 - t_8)$; $t_{10} = (u_{11} + u_{10})(t_1 + t_2 - t_6)$, $t_{11} = u_{10}(t_2 - t_6)$;	11M+2SQ
2	compute resultant res_1 of w_1 and u_1, and $z_1 := res_1/w_1 \bmod u_1$ $t_{12} = -u_{10}t_1$, $t_{13} = u_{11}(t_6 - t_2)$; $t_{14} = u_{12}(t_7 + t_8 - t_4 - 1)$, $t_{15} = u_{10}(t_7 + t_8 - t_4 - 1)$; $t_{16} = u_{11}(t_9 + t_{10} - t_5 - f_3 - t_7 - t_{11})$; $t_{17} = u_{12}(t_9 + t_{10} - t_5 - f_3 - t_7 - t_{11})$; $s_3 = (t_{12} + t_5 + f_3 + t_7 + t_{11} - t_9 - t_{10})^2$; $s_4 = (t_4 + 1 - 2t_7 - t_8)^2$, $t_{18} = (t_2 - 2t_6)(t_{15} - t_{16})$; $t_{19} = (t_{12} + t_{13} + t_5 + f_3 + t_7 + t_{11} - t_9 - t_{10} - t_{14})(s_3 - t_{18})$; $t_{20} = (t_2 - 2t_6)(-t_{11} - t_{17})$; $t_{21} = (t_4 + 1 - 2t_7 - t_8)(t_5 + t_{12} + t_7 + f_3 + t_{11} - t_9 - t_{10})$; $t_{22} = (t_{20} - 2t_{21})(-t_{11} - t_{17})$, $t_{23} = (t_{15} - t_{16})s_4$; $res_1 = t_{19} + t_{22} + t_{23}$; $t_{24} = (t_2 - 2t_6)(t_{13} + t_{12} + t_7 + t_{11} + t_5 + f_3 - t_9 - t_{10} - t_{14})$; $inv_0 = t_{24} - s_4$, $t_{25} = u_{12} \cdot inv_0$; $t_{26} = u_{12}(t_{20} - t_{21})$, $t_{27} = u_{11} \cdot inv_0$; $inv_1 = t_{25} + t_{21} - t_{20}$, $inv_2 = t_{27} + t_{18} - t_{26} - s_3$; $z_1 = inv_0x^2 + inv_1x + inv_2$	16M+2SQ
3	compute the cubic $w = y^2 + sy + t$ $t_{28} = v_{12}v_{11}$, $t_{29} = v_{11}v_{10}$, $s_5 = v_{10}^2$; $t_{30} = u_{12}s_1$, $t_{31} = u_{11}s_1$, $t_{32} = u_{12}(t_{30} - 2t_{28})$; $t_{33} = (u_{11} + u_{10})(s_1 + 2t_{28} - t_{30})$; $t_{34} = u_{10}(t_{30} - 2t_{28})$; $t_{35} = (t_{32} + 2t_3 + s_2 - t_{31})inv_0$; $t_{36} = (2t_{29} + t_{31} - t_{33} - t_{34})inv_1$; $t_{37} = (s_5 + t_{34})inv_2$; $t_{38} = (t_{32} + s_2 + 2t_3 + 2t_{29} - t_{33} - t_{34})(inv_0 + inv_1)$; $t_{39} = (t_{32} + t_{34} + s_2 + s_5 + 2t_3 - t_{31})(inv_0 + inv_2)$; $t_{40} = (t_{31} + s_5 + 2t_{29} - t_{33})(inv_1 + inv_2)$; $t_{41} = u_{12}t_{35}$, $t_{42} = u_{11}t_{35}$; $t_{43} = u_{12}(t_{41} + t_{36} + t_{35} - t_{38})$; $t_{44} = (u_{11} + u_{10})(t_{38} - t_{41} - t_{36})$; $t_{45} = u_{10}(t_{41} + t_{36} + t_{35} - t_{38})$; $r_0 = t_{43} + t_{39} + t_{36} - t_{42} - t_{35} - t_{37}$; $r_1 = t_{40} + t_{42} - t_{36} - t_{37} - t_{44} - t_{45}$; $r_2 = t_{37} + t_{45}$, $t_{46} = res_1r_0$, $t_{47} = r_0s_1$; $t_{48} = t_{47}res_1$, $t_{49} = -2res_1v_{12}$, $t_{50} = 3r_1s_1$; $t_{51} = 3t_{47}u_{12}$, $\gamma_1 = t_{51} - t_{49} - t_{50})$; $t_{52} = res_1\gamma_1$, $t_{53} = -t_{46}v_{11}$, $t_{54} = -t_{46}v_{10}$; $t_{55} = r_1\gamma_1$, $t_{56} = 3r_2t_{47}$, $t_{57} = r_2\gamma_1$; $t_{58} = 3t_{47}u_{11}$, $t_{59} = 3t_{47}u_{10}$; $t_{60} = t_{58}r_0$, $t_{61} = t_{59}r_0$; $\lambda_1 = 3(2t_{53} + t_{55} + t_{56} - t_{60})$; $\mu_1 = 3(2t_{54} + t_{57} - t_{61})$, $t_{62} = -3t_{46}v_{12}$; $t_{63} = -(v_{12} + v_{11})(\lambda_1 - t_{62} - 3t_{53})$; $t_{64} = -v_{11}(\lambda_1 - 3t_{53})$; $t_{65} = -(v_{12} + v_{10})(\mu_1 - t_{62} - 3t_{54})$; $t_{66} = -v_{10}(\mu_1 - 3t_{54})$; $t_{67} = -(v_{11} + v_{10})(\lambda_1 + \mu_1 - 3t_{53} - 3t_{54})$; $t_{68} = 3t_{48}(u_{12} + u_{11})$, $t_{69} = 3t_{48}u_{11}$; $t_{70} = (u_{12} + u_{10})t_{52}$, $t_{71} = u_{10}t_{52}$; $t_{72} = (u_{11} + u_{10})(3t_{48} + t_{52})$; $B_0 = t_{52} + t_{68} + t_{63} + 3t_{48} - t_{69} - t_{64}$; $B_1 = t_{70} + t_{69} + t_{65} + t_{64} + 3t_{48} - t_{71} - t_{66}$; $B_2 = t_{72} + t_{67} - t_{69} - t_{71} - t_{64} - t_{66}$; $B_3 = t_{71} + t_{66}$, $t_{73} = 3t_{46}B_0$, $i_1 = (t_{73})^{-1}$; $t_{74} = i_1B_0$, $t_{75} = 3t_{46}i_1$, $t_{76} = 3t_{46}t_{75}$; $t_{77} = t_{75}B_1$, $t_{78} = t_{75}B_2$, $t_{79} = t_{75}B_3$; $t_{80} = t_{74}\lambda_1$, $t_{81} = t_{74}\mu_1$, $t_{82} = t_{74}B_0$; $t_{83} = t_{74}B_1$, $t_{84} = t_{74}B_2$, $t_{85} = t_{74}B_3$; $w = y^2 + (t_{80}x + t_{81})y + t_{82}x^3 + t_{83}x^2 + t_{84}x + t_{85}$	58M+1SQ+1I

4	compute $res(w,C,y)$ $s_6 = t_{77}^2$, $t_{86} = t_{77}(6t_{78} + s_6)$, $s_7 = t_{80}^2$; $s_8 = (t_{80} + t_{81})^2$, $s_9 = t_{81}^2$, $t_{87} = t_{80}t_{82}$; $t_{88} = t_{80}(s_7 - 3t_{83})$, $t_{89} = t_{81}t_{82}$, $t_{90} = -3f_3t_{87}$; $t_{91} = t_{80}(s_8 - 3t_{84} - s_7 - s_9)$, $t_{92} = t_{81}(s_7 - 3t_{83})$; $t_{93} = f_3t_{88}$, $t_{94} = -3f_2t_{87}$, $t_{95} = -3f_3t_{89}$, $s_{10} = t_{76}^2$; $t_{96} = t_{76}s_{10}$, $t_{97} = t_{96}(1 - 3t_{87})$; $t_{98} = t_{96}(t_{88} + t_{90} + 2f_3 - 3t_{89})$; $t_{99} = t_{96}(t_{91} + t_{92} + t_{93} + t_{94} + t_{95} + 2f_2 + f_3^2)$;	14M+5SQ
5	compute u_{-2D_1} $s_{11} = u_{12}^2$, $t_{100} = u_{12}u_{11}$; $t_{101} = (2u_{11} + 2u_{10} + 2t_{100} + s_{11})(1 + t_{97} + 3t_{77} - 2u_{12})$; $t_{102} = (2u_{10} + 2t_{100})(t_{97} + 3t_{77} - 2u_{12})$; $c_1 = t_{97} + 3t_{77} - 2u_{12}$, $t_{103} = 2u_{12}c_1$; $c_2 = t_{98} + 3t_{78} + 3s_6 - s_{11} - t_{103} - 2u_{11}$; $t_{104} = 2u_{12}c_2$; $c_3 = 2u_{11} + s_{11} + t_{102} + t_{99} + t_{86} + 3t_{79} - t_{104} - t_{101}$; $u_{-(2D_1)} = x^3 + c_1x^2 + c_2x + c_3$	5M+1SQ
6	compute $res(t - s^2, u_{-2D_1}, x)$ and precomputations for v_{2D_1} $t_{105} = c_3t_{82}$, $t_{106} = c_1t_{82}$, $t_{107} = c_2t_{82}$; $t_{108} = c_2(t_{83} - s_7)$, $t_{109} = c_1(t_{84} + s_7 + s_9 - s_8)$; $t_{110} = c_3(t_{84} + s_7 + s_9 - s_8)$, $t_{111} = c_2(t_{85} - s_9)$; $t_{112} = c_3(t_{83} - s_7)$, $t_{113} = c_1(t_{85} - s_9)$; $s_{12} = (t_{105} + s_9 - t_{85})^2$; $s_{13} = (t_{107} + s_8 - t_{84} - s_7 - s_9)^2$; $t_{114} = (t_{106} + s_7 - t_{83})(t_{110} - t_{111})$; $t_{115} = (t_{105} + t_{108} + s_9 - t_{85} - t_{109})(s_{12} - t_{114})$; $t_{116} = (t_{112} - t_{113})(t_{106} + s_7 - t_{83})$; $t_{117} = (t_{107} + s_8 - t_{84} - s_7 - s_9)(t_{105} + s_9 - t_{85})$; $t_{118} = (t_{112} - t_{113})(t_{116} - 2t_{117})$; $t_{119} = (t_{110} - t_{111})s_{13}$, $res_2 = t_{115} + t_{118} + t_{119}$; $t_{120} = (t_{108} + s_9 + t_{105} - t_{109} - t_{85})(t_{106} - t_{83} + s_7)$; $j_0 = t_{120} - s_{13}$, $t_{121} = j_0 \cdot c_1$; $t_{122} = c_1(t_{116} - t_{117})$, $t_{123} = j_0 \cdot c_2$; $j_1 = t_{121} + t_{117} - t_{116}$, $j_2 = t_{123} + t_{114} - t_{122} - s_{12}$; $t_{124} = t_{80}(t_{83} + t_{84})$, $t_{125} = t_{80}t_{84}$; $t_{126} = t_{81}(t_{83} + t_{85})$, $t_{127} = t_{81}t_{85}$; $t_{128} = (t_{80} + t_{81})(t_{84} + t_{85})$, $t_{129} = c_1(1 - t_{87})$; $t_{130} = (t_{129} + t_{89} + t_{124} - f_3 - t_{125})c_1$; $t_{131} = c_2(1 - t_{87})$; $t_{132} = (c_2 + c_3)(1 + f_3 + t_{125} - t_{87} - t_{129} - t_{89} - t_{124})$; $t_{133} = c_3(t_{129} + t_{89} + t_{124} - f_3 - t_{125})$; $t_{134} = (t_{130} + f_2 + t_{127} - t_{131} - t_{126} - t_{125})j_0$; $t_{135} = (j_0 + j_1)(t_{130} + f_2 + f_1 + 2t_{127} - t_{126} - t_{128} - t_{132} - t_{133})$; $t_{136} = (f_1 + t_{125} + t_{127} + t_{131} - t_{128} - t_{132} - t_{133})j_1$; $t_{137} = (j_0 + j_2)(t_{130} + t_{133} + f_2 + f_0 - t_{131} - t_{126} - t_{125})$; $t_{138} = (f_0 + t_{133} - t_{127})j_2$; $t_{139} = (j_1 + j_2)(f_1 + f_0 + t_{125} + t_{131} - t_{128} - t_{132})$; $t_{140} = t_{134}c_1$, $t_{141} = c_2t_{134}$; $t_{142} = c_1(t_{140} + t_{134} + t_{136} - t_{135})$; $t_{143} = (c_2 + c_3)(t_{135} - t_{140} - t_{136})$; $t_{144} = c_3(t_{140} + t_{134} + t_{136} - t_{135})$;	40M+2SQ
7	compute v_{2D_1} $t_{145} = res_2(t_{142} + t_{137} + t_{136} - t_{141} - t_{134} - t_{138})$; $i_2 = (t_{145})^{-1}$; $t_{146} = i_2(t_{142} + t_{137} + t_{136} - t_{141} - t_{134} - t_{138})$; $t_{147} = t_{146}(t_{142} + t_{137} + t_{136} - t_{141} - t_{134} - t_{138})$; $t_{148} = t_{146}(t_{139} + t_{141} - t_{136} - t_{138} - t_{143} - t_{144})$; $t_{149} = t_{146}(t_{138} + t_{144})$; $v_2' = -t_{147}$, $v_1' = -t_{148}$, $v_0' = -t_{149}$;	5M+1I
8	compute u_{2D_1} $s_{14} = res_2^2$, $t_{150} = i_2s_{14}$, $s_{15} = t_{150}^2$; $t_{151} = t_{150}s_{15}$, $t_{152} = t_{150}t_{148}$, $s_{16} = t_{152}^2$; $t_{153} = t_{150}t_{149}$, $t_{154} = t_{152}(s_{16} + 6t_{153})$; $t_{155} = t_{151}f_3$, $t_{156} = c_1(3t_{152} - c_1)$; $d_1 = 3t_{152} - c_1$, $d_2 = 3t_{153} + 3s_{16} + t_{151} - c_2 - t_{156}$; $t_{157} = c_1d_2$, $t_{158} = c_2(3t_{152} - c_1)$; $d_3 = t_{154} + t_{155} - t_{157} - c_3 - t_{158}$;	9M+3SQ
total		158M, 16S, 2I