コンピュータセキュリティ　14−12
(2001. 7. 25)

非特異代数曲線のヤコビアン群演算に関する一考察*

原澤　隆一

大阪大学
560-0043, 大阪府豊中市待兼山町 1-1
E-mail: harasawa@math.sci.osaka-u.ac.jp

あらまし　本論文の目的は、有限体上定義された非特異代数曲線のヤコビアン群演算の効率的な方法を述べることである。

ヤコビアン群演算の効率的アルゴリズムの提案は、代数曲線暗号を考察する上で非常に大事な項目である。g を曲線の種数としたとき、実用化が進められたいる (超) 楕円曲線暗号においては、そのヤコビアン群演算が $O(g^2)$ 回の定義体上の演算で実行される。また、C_{ab} 曲線においても、原澤, 鈴木らが $O(g^2)$ で実行可能なヤコビアン群演算アルゴリズムを提案した。本論文では、その方法が、より一般的な $C_{a_1,\cdots,a_t}$ 曲線に拡張できることを示す。さらに、この計算量が $O(g^2)$ となることもわかる。

また、この拡張は代数曲線暗号の観点において、全ての曲線に適用できることもわかる。

キーワード　代数曲線暗号, ヤコビアン群演算, イデアル類群, $C_{a_1,\cdots,a_t}$ 曲線

*日本学術振興会科学研究費補助金による研究成果

A Remark on Jacobian Group Arithmetic on Nonsingular Algebraic Curves *

Ryuichi Harasawa

Osaka Univresity
560-0043, 1-1 Machikaneyama, Toyonaka-si, Osaka
E-mail: harasawa@math.sci.osaka-u.ac.jp

Abstract　The aim of this paper is to describe a method that gives an efficient algorithm for performing Jacobian group arithmetic on the most general algebraic curves over finite fields. When we consider algebraic curve cryptosystems, an efficient Jacobian group arithmetic is required. For elliptic and hyperelliptic curve cryptosystems, there exist algorithms for performing the Jacobian group arithmetic in $O(g^2)$ operations in the base field, where g is the genus of a curve. Furthermore, for more general curves so-called C_{ab} curves, R.Harasawa and J.Suzuki proposed a method for performing the Jacobian group arithmetic in $O(g^2)$ operations in the base field. We generalize the method to $C_{a_1,\cdots,a_t}$ curves. Furthermore, it turns out that the generalization gives an efficient algorithm for performing Jacobian group arithmetic in $O(g^2)$ operations in the base field for all algebraic curves that we consider from an algebraic curve cryptographical point of view.

key words　algebraic curve cryptography, Jacobian group arithmetic, ideal class group, $C_{a_1,\cdots,a_t}$ curves

*Research supported by a science research grant of the Japan Society for the Promotion of Science

1 Introduction

The aim of this paper is to describe a method that gives an efficient algorithm for performing Jacobian group arithmetic on the most general algebraic curves for which cryptosystems based on the intractability of the discrete logarithm problem (DLP) can be cosidered.

When we consider algebraic curve cryptosystems, an efficient Jacobian group arithmetic is required. For elliptic, hyperelliptic and C_{ab} curve, there exist some algorithm for performing the Jacobian group arithmetic in $O(g^2)$ operations in the base field ([11] [12] [7]), where g is the genus of a curve. However, it is also a fact that there exist some attacks against the DLP on these curves ([8] [5] [1] [6] [3] etc.). Therefore, it is important to consider cryptosystems based on more general curves than C_{ab} curves.

In this paper, we address the problem whether or not there exists a method for performing Jacobian group arithmetic in $O(g^2)$ operations in the base field for the most general curves. Now we consider nonsingular curves satisfying the following condition [9]:

the set of pole numbers of the point at infinity is generated by t elements $< a_1, \cdots, a_t >$.

We call the curves $C_{a_1,\cdots,a_t}$ curves. Particularly, in the case of $t = 2$, the curve are C_{ab} curves, which include elliptic and hyperelliptic curves. A difference between previous curves and $C_{a_1,\cdots,a_t}$ curves is that the number of the definition equation is not necessarily one.

In this paper, we generalize Harasawa et al.'s method [7] for C_{ab} curves to $C_{a_1,\cdots,a_t}$ curves, so that there does exist a method which performs Jacobian group arithmetic on $C_{a_1,\cdots,a_t}$ curves in $O(g^2)$ operations in the base field in the case that the sizes of a_1 and the base field are fixed.

We note that, for $C_{a_1,\cdots,a_t}$ curves, S.Arita has already proposed an algorithm for performing the Jacobian group arithmetic, which takes $O(g^3)$ operations in the base field [2].

Finally, S. Miura [9] showed that all nonsingular curves C defined over a perfect field K (especially, a finite field) with at least one K-rational point are $C_{a_1,\cdots,a_t}$ curves. Therefore, from an algebraic curve cryptographical point of view, it turns out that this proposed method gives an efficient algorithm for performing Jacobian group arithmetic in $O(g^2)$ field operations for all algebraic curves C/K, since we consider curves with only one K-rational point at infinity.

2 $C_{a_1,\cdots,a_t}$ curves

The notation follows [13].

Let $\mathbf{A}_t \subset \mathbf{N}_0$ be a monoid generated by $a_1, \cdots, a_t \in \mathbf{N}_0$ with $a_i < a_{i+1}$ (i.e. $\mathbf{A}_t := < a_1, \cdots, a_t > = a_1\mathbf{N}_0 + \cdots + a_t\mathbf{N_0}$), where $\mathbf{N}_0$ is the set of non-negative integers.

From now on, we assume that $\mathbf{A}_t = < a_1, \cdots, a_t >$ is represented as a minimum generating system (i.e. , $a_i \notin < a_1, \cdots, a_{i-1}, a_{i+1}, \cdots, a_t >$ for $1 \leq \forall i \leq t$) and $\gcd(a_1, \cdots, a_t) = 1$.

And we define $\Psi_{\mathbf{A}_t} : \mathbf{N}_0^t \longrightarrow \mathbf{N}_0$ as $\Psi_{\mathbf{A}_t}(n_1, \cdots, n_t) = \sum_{i=1}^{t} a_i n_i$.

Now, we define an ordering on $\mathbf{N}_0^t$ as follows[9]:

Definition 1 ($C_{a_1,\cdots,a_t}$ **order**) *We say* $\alpha >_{a_1,\cdots,a_t} \beta$ *for* $\alpha = (\alpha_1, \cdots, \alpha_t), \beta = (\beta_1, \cdots, \beta_t) \in \mathbf{N}_0^t$ *if one of the following two conditions holds:*

1. $\Psi_{\mathbf{A}_t}(\alpha_1, \cdots, \alpha_t) > \Psi_{\mathbf{A}_t}(\beta_1, \cdots, \beta_t)$, *or*
2. $\Psi_{\mathbf{A}_t}(\alpha_1, \cdots, \alpha_t) = \Psi_{\mathbf{A}_t}(\beta_1, \cdots, \beta_t)$, $\alpha_1 = \beta_1, \cdots, \alpha_i = \beta_i, \alpha_{i+1} < \beta_{i+1}$.

In this paper, we call the ordering $C_{a_1,\cdots,a_t}$ *order.*

Next we define two sets $\mathbf{B}(\mathbf{A}_t)$ and $\mathbf{V}(\mathbf{A}_t)$ as follows:

$$\mathbf{B}(\mathbf{A}_t) := \{ \text{ the least M} \in \mathbf{N}_0^t \text{ with respect to } C_{a_1,\cdots,a_t} \text{ order with } \Psi_{\mathbf{A}_t}(\mathrm{M}) = a | \ a \in \mathbf{A}_t \},$$

$$\mathbf{V}(\mathbf{A}_t) := \{\mathrm{L} \in \mathbf{N}_0^t \setminus \mathbf{B}(\mathbf{A}_t) |\ \mathrm{L=M+N},\ \mathrm{M} \in \mathbf{N}_0^t \setminus \mathbf{B}(\mathbf{A}_t), \mathrm{N} \in \mathbf{N}_0^t \Rightarrow \mathrm{N}=(0,\cdots,0)\}.$$

Then, the following theorem is known:

Theorem 1 ($C_{a_1,\cdots,a_t}$ **curve [9])** *Let C be an algebraic curve defined over a perfect field K with a K-rational point P. And we define $\mathbf{M}_P$ as the set of pole numbers of P (i.e. $\mathbf{M}_P = \{-v_P(f) |\ f \in L(\infty P)\}$, where $L(\infty P) := \cup_i L(iP)$ for $P \in C$).*

Then , if

$$\mathbf{M}_P = \mathbf{A}_t =< a_1, \cdots, a_t >$$

holds, the curve C has a nonsingular affine model in t variables with the defining equations:

$$\{F_{\mathbf{M}} = 0 |\ \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\},$$

$$F_{\mathbf{M}} = X^{\mathbf{M}} + \alpha_{\mathbf{L}} X^{\mathbf{L}} + \sum_{\mathbf{N} \in \mathbf{B}(\mathbf{A}_t), \Psi_{\mathbf{A}_t}(\mathbf{N}) < \Psi_{\mathbf{A}_t}(\mathbf{L})} \alpha_{\mathbf{N}} X^{\mathbf{N}}, \tag{1}$$

where we denote $\prod_i X_i^{\mathbf{m}_i}$ by $X^{\mathbf{M}}$ for $\mathbf{M} = (\mathbf{m_1}, \cdots, \mathbf{m_t}) \in \mathbf{N}_0^t$, and $X_i \in L(\infty P)$ is a function such that $(X_i)_\infty = a_i P$.

Here, $\mathbf{L}$ is the unique $\mathbf{L} \in \mathbf{B}(\mathbf{A}_t)$ satisfying $\Psi_{\mathbf{A}_t}(\mathbf{M}) = \Psi_{\mathbf{A}_t}(\mathbf{L})$, and $\alpha_{\mathbf{L}} \neq 0, \alpha_{\mathbf{N}} \in K$.

Furthermore, P is only one point at infinity.

In this paper, we call the affine curve $\{F_{\mathbf{M}} = 0 |\ \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\}$ a "$C_{a_1,\cdots,a_t}$ curve".

Example 1 ($C_{3,5,7}$ **Curve)** *$C_{3,5,7}$ curve C is defined by three equations as follows:*

$$\begin{cases} Y^2 &= r_1XZ + r_2X^3 + r_3XY + r_4Z + r_5X^2 + r_6Y + r_7X + r_8 \\ YZ &= s_1X^4 + s_2X^2Y + s_3XZ + s_4X^3 + s_5XY + s_6Z + s_7X^2 + s_8Y + s_9X + s_{10} \\ Z^2 &= t_1X^3Y + t_2X^2Z + t_3X^4 + t_4X^2Y + t_5XZ + t_6X^3 + t_7XY + t_8Z + t_9X^2 \\ & \quad + t_{10}Y + t_{11}X + t_{12}, \end{cases}$$

where $(X)_\infty = 3P$, $(Y)_\infty = 5P$, $(Z)_\infty = 7P$, and r_1, s_1 and t_1 are nonzero elements.

It is known [9] that the genus of a $C_{a_1,\cdots,a_t}$ curve is given by

$$g = \#(\mathbf{N}_0 \setminus \mathbf{A}_t) = \sum_{i=0}^{a_1-1} \lfloor b_i/a_1 \rfloor, \tag{2}$$

where $b_i := \min\{b \in < a_2, \cdots, a_t > |\ b \equiv i \pmod{a_1}\}$
and $\lfloor b_i/a_1 \rfloor := \max\{s \in \mathbf{Z} |\ s \leq b_i/a_1\}$.

From now on, we assume K to be a finite field $\mathbf{F}_q$ with q elements.

Remark 1 *From an algebraic curve cryptographical point of view, it is sufficient that only $C_{a_1,\cdots,a_t}$ curves be examined, since we suppose that a curve C/K has only one K-rational point at infinity, which is a $C_{a_1,\cdots,a_t}$ curve from Theorem 1.*

3 Jacobian group arithmetic on $C_{a_1,\cdots,a_t}$ Curves

Since $C_{a_1,\cdots,a_t}$ curves C are nonsingular and have only one K-rational point at infinity, the Jacobian group $J_K(C)$ is isomorphic to the ideal class group $Cl(R)$ of the coordinate ring $R := K[x_1, \cdots, x_t]$, where $x_i \equiv X_i \bmod (F_{\mathbf{M}} = 0 |\ \mathbf{M} \in \mathbf{V}(\mathbf{A}_t))$. And we define $x^m := \prod_i x_i^{m_i}$ for $m = (m_1, \cdots, m_t) \in \mathbf{N}_0^t$.

And, for each element in $J_K(C)$, there exists a divisor of the form $E - nP$ with $E \geq 0$ and $P \notin \mathrm{support}(E)$, which is said to be a semi-reduced divisor.

Furthermore, if n is minimized in $D_1 = E - nP$ with $E \geq 0$ and $P \notin \mathrm{support}(E)$ (semi-reduced) and $D_1 \sim D \in \mathrm{Div}_K^0(C)$, then D_1 is said to be the reduced divisor equivalent to D. For a reduced divisor $D = E - nP$, it holds $n \leq g$. And the reduced divisor is unique for each element of $J_K(C)$.

The isomorphism Φ between $J_K(C)$ and $Cl(R)$ is given as follows:

$$\Phi : J_K(C) \to Cl(R),$$

$$[\sum_{Q \in C, Q \neq P} n_Q Q - (\sum_{Q \in C, Q \neq P} n_Q) P] \mapsto [L(\infty P - (\sum_{Q \in C, Q \neq P} n_Q) Q)], \tag{3}$$

where we denote the ideal class which ideal $I \subset K[x_1, \cdots, x_t]$ belongs to by $[I]$.

We call the ideals corresponding to reduced and semi-reduced divisors the reduced and semi-reduced ideals, respectively. Then each semi-reduced ideal I is expressed by an integral ideal $I \subset L(\infty P) = K[x_1, \cdots, x_t]$. And, for a semi-reduced ideal I, we define the degree of I by such an n that $E - nP$ with $E \geq 0$ and $P \notin \mathrm{support}(E)$ is a semi-reduced divisor that corresponds to I.

From now on, we consider the arithmetic on the Jacobian group as that on the ideal class group of the coordinate ring.

Here, we introduce the propety of the coordinate ring of $C_{a_1,\cdots,a_t}$ curve:

Theorem 2 *[9] If we define* $\mathbf{T}(\mathbf{A}_t)$ *as* $\mathbf{T}(\mathbf{A}_t) = \mathbf{B}(\mathbf{A}_t) \cap \{0\} \times \mathbf{N}^{t-1}$, *then it holds* $\mathbf{T}(\mathbf{A}_t) = \{\mathbf{M}(b_i) | \ 0 \leq i \leq a_1 - 1\}$ *and* $\#\mathbf{T}(\mathbf{A}_t) = a_1$, *where* b_i *is the same as in (2) and* $\mathbf{M}(b_i) \in \mathbf{N}_0^t$ *is the minimal element* $\mathbf{M}$ *satisfying* $\Psi_{\mathbf{A}_t}(\mathbf{M}) = b_i$ *with respect to* $C_{a_1,\cdots,a_t}$ *order.*

Furthermore, $\{x^{\gamma_0} = 1, x^{\gamma_1}, \cdots, x^{\gamma_{a_1-1}}\}$ *is a* $K[x_1]$*-basis of the coordinate ring* $R = K[x_1, \cdots x_t]$, *where* $\{\gamma_0, \cdots, \gamma_{a_1-1}\}$ *are the elements of* $\mathbf{T}(\mathbf{A}_t)$.

Now, for each integral ideal of R, the $K[x_1]$-basis can be uniquely expressed by taking the Hermite normal form (HNF) of the matrix $(\beta_{i,j})$, where the $K[x_1]$-basis is given as the matrix $(\beta_0, \cdots, \beta_{a_1-1})$ with $\beta_k = \sum_{l=0}^{a_1-1} \beta_{l,k}(x_1) x^{\gamma_l}$, since the coordinatering R is a $K[x_1]$-module.

Therefore, we express each representative element (i.e. reduced ideal) in an ideal class group of R by the HNF of the $K[x_1]$-basis.

Furthermore, it turns out that the degree of an ideal is equal to the degree of x_1 in the product of the diagonal elements of the HNF (see Appendix).

Here, it is known that we can obtain the Jacobian group arithmetic on $C_{a_1,\cdots,a_t}$ curves as follows:

Algorithm 1 (Jacobian group arithmetic on $C_{a_1,\cdots,a_t}$ curves)

[Each ideal is expressed by the Hermite normal form.]

Input: *Reduced ideals* I_1, I_2 *in* R (HNF).

Output: *The reduced ideal* $I_3 \sim I_1 I_2$ (HNF).

Step 1: $D \leftarrow I_1 I_2$;

Step 2: $J \leftarrow$ *a semi-reduced ideal s.t.* $D^{-1} = \frac{J}{(e)}$, *where* (e) *is a principal ideal generated by* $e \in K[x_1]$ *(then, it holds* $J \sim D^{-1}$*);*

Step 3: $f \leftarrow$ *a minimal nonzero element in* J *with respect to* $-v_P(\cdot)$;

Step 4: $I_3 \leftarrow$ *the* HNF *of* $(f)J^{-1} = \frac{(f)D}{(e)}$.

In order to compute the description of Algorithm 1, we should fix the following procedures:

1. how to compute the inverse ideal I^{-1} given an ideal I (Step 2); and
2. how to compute the minimal element over an ideal with respect to $-v_P(\cdot)$ (Step 3).

4 Proposed Method

In this section, we propose the method for performing the Jacobian group arithmetic on $C_{a_1,\cdots,a_t}$ curves (Algorithm 1).

4.1 Computing Inverse Ideal

Let $K(C)$ be the function field of a $C_{a_1,\cdots,a_t}$ curve C.

From the fact that the integral closure of $K(C)$ over $K[x_1]$ is the coordinate ring R and the integral basis is $\{x^{\gamma_i}\}_{0\leq i\leq a_1-1}$, we can extend a method [4] of number fields in a natural manner.

Then, we can compute an inverse ideal if we can compute the matrix $T = (t_{i,j})_{0\leq i,j\leq a_1-1} = (Tr_{K(C)/K(x_1)}(x^{\gamma_i}x^{\gamma_j}))_{0\leq i,j\leq a_1-1}$ [7].

And it is sufficient to compute only $Tr_{K(C)/K(x_1)}(x^{\gamma_i})$, since
$Tr_{K(C)/K(x_1)}(x^{\gamma_i}x^{\gamma_j}) = Tr_{K(C)/K(x_1)}(\sum_{0\leq k\leq a_1-1} g_k^{(i,j)}(x_1)x^{\gamma_k}) = \sum_{0\leq k\leq a_1-1} g_k^{(i,j)}(x_1)Tr_{K(C)/K(x_1)}(x^{\gamma_k})$,
where $x^{\gamma_i}x^{\gamma_j} := \sum_{0\leq k\leq a_1-1} g_k^{(i,j)}(x_1)x^{\gamma_k}$.

Here, for C_{ab} curves $\sum_{0\leq i\leq b,0\leq j\leq a,ai+bj\leq ab}\alpha_{i,j}x^iy^j = 0$, since the integral basis is $\{y^i\}_{0\leq i\leq a-1}$, we can compute the values of $Tr_{K(C)/K(x)}(y^i)$ as follows [7]:

1. $Tr_{K(C)/K(x)}(y)$ can be obtained if the minimal polynomial of y over $K[x]$ is given, which coincides with the definition equation;
2. $Tr_{K(C)/K(x)}(y^i)$ can be computed by using the minimal polynomial of y over $K[x]$ and the Newton formula (page 163, [4]).

However, generally, given an integral basis, it is not obvious to compute the minimal polynomial.
Now, we proposed a method of computing the minimal polynomial of each x^{γ_i} over $K[x_1]$.
First, for extension degrees of x^{γ_i} over $K[x_1]$, we show the folloing proposition.

Proposition 1 *For* $1 \leq i \leq a_1 - 1$, *it holds*

$$[K(x_1, x^{\gamma_i}) : K(x_1)] = \frac{a_1}{l},$$

where $l := \gcd(i, a_1) = \gcd(\Psi_{\mathbf{A}_t}(\gamma_i), a_1)$.

Proof of Proposition 1
It is sufficient to show $[K(C) : K(x_1, x^{\gamma_i})] = l$, since $a_1 = \deg(x_1)_\infty = [K(C) : K(x_1)] = [K(C) : K(x_1, x^{\gamma_i})][K(x_1, x^{\gamma_i}) : K(x_1)]$,
Now, it holds $\Psi_{\mathbf{A}_t}(\gamma_i) = \deg(x^{\gamma_i})_\infty = [K(C) : K(x^{\gamma_i})] = [K(C) : K(x_1, x^{\gamma_i})][K(x_1, x^{\gamma_i}) : K(x^{\gamma_i})]$, which implies $[K(C) : K(x_1, x^{\gamma_i})] | \gcd(a_1, \Psi_{\mathbf{A}_t}(\gamma_i)) = \gcd(a_1, i) = l$.
Therefore, the Proposition holds if $l = 1$.
We consider the case of $l > 1$ (,especially $i \neq 1$).
Now we suppose that $m := [K(C) : K(x_1, x^{\gamma_i})] < l$.
And we define the minimal polynomial $F(x_1, x^{\gamma_i}, x^{\gamma_1}) = 0$ of $x^{\gamma_1} \in K(C)$ over $K(x_1, x^{\gamma_i})$ as

$$F(x_1, x^{\gamma_i}, x^{\gamma_1}) = \sum_{0\leq j\leq m', f_j(x_1,x^{\gamma_i})\neq 0} f_j(x_1, x^{\gamma_i})(x^{\gamma_1})^j, \tag{4}$$

where $f_j(x_1, x^{\gamma_i}) \in K[x_1, x^{\gamma_i}]$.
Then it holds $-v_P(f_j(x_1, x^{\gamma_i})(x^{\gamma_1})^j) \equiv j \pmod{l}$, which implies

$$-v_P(F(x_1, x^{\gamma_i}, x^{\gamma_1})) = \max_{j, f_j(x_1,x^{\gamma_i})\neq 0}\{-v_P(f_j(x_1, x^{\gamma_i})(x^{\gamma_1})^j)\} < \infty,$$

since $j < m' \leq m < l$ and $-v_P(x^{\gamma_1}) \equiv 1 \pmod{l}$. It contradicts $v_P(0) = \infty$.

Hence $[K(C) : K(x_1, x^{\gamma_i})] = l$. **Q.E.D.**

From Proposition 1, we can compute $Tr_{K(C)/K(x_1)}(x^{\gamma_i})$ as follows:

Stage 1 if $i = 0$ then $Tr_{K(C)/K(x_1)}(x^{\gamma_i}) \leftarrow a_1$, otherwise $m \leftarrow \frac{a_1}{l}$ with $l = \gcd(i, a_1)$;

Stage 2 the computation of $(f_j^i(x_1))$ with

$$\begin{bmatrix} 1 \\ x^{\gamma_i} \\ \vdots \\ (x^{\gamma_i})^{m-1} \\ (x^{\gamma_i})^m \end{bmatrix} = \begin{bmatrix} f_0^0(x_1) & f_1^0(x_1) & \cdots & f_{a_1-2}^0(x_1) & f_{a_1-1}^0(x_1) \\ f_0^1(x_1) & f_1^1(x_1) & \cdots & f_{a_1-2}^1(x_1) & f_{a_1-1}^1(x_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ f_0^{m-1}(x_1) & f_1^{m-1}(x_1) & \cdots & f_{a_1-2}^{m-1}(x_1) & f_{a_1-1}^{m-1}(x_1) \\ f_0^m(x_1) & f_1^m(x_1) & \cdots & f_{a_1-2}^m(x_1) & f_{a_1-1}^m(x_1) \end{bmatrix} \begin{bmatrix} 1 \\ x^{\gamma_1} \\ \vdots \\ x^{\gamma_{a_1-2}} \\ x^{\gamma_{a_1-1}} \end{bmatrix}$$

Stage 3 the computation of minimal polynomial

$D(x_1, x^{\gamma_i}) = (x^{\gamma_i})^m + \sum_{0 \leq j \leq m-1} D_j^{(i)}(x_1)(x^{\gamma_i})^j$ with

$$\left[\begin{array}{c|cccc} * & * & \cdots & * & * \\ * & * & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & \cdots & * & * \\ D(x_1, x^{\gamma_i}) & 0 & \cdots & 0 & 0 \end{array}\right]$$

by performing elementary operations on rows from

$$\left[\begin{array}{c|cccc} 1 & f_0^0(x_1) & f_1^0(x_1) & \cdots & f_{a_1-2}^0(x_1) & f_{a_1-1}^0(x_1) \\ x^{\gamma_i} & f_0^1(x_1) & f_1^1(x_1) & \cdots & f_{a_1-2}^1(x_1) & f_{a_1-1}^1(x_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (x^{\gamma_i})^{m-1} & f_0^{m-1}(x_1) & f_1^{m-1}(x_1) & \cdots & f_{a_1-2}^{m-1}(x_1) & f_{a_1-1}^{m-1}(x_1) \\ (x^{\gamma_i})^m & f_0^m(x_1) & f_1^m(x_1) & \cdots & f_{a_1-2}^m(x_1) & f_{a_1-1}^m(x_1) \end{array}\right]$$

Stage 4 $Tr_{K(C)/K(x_1)}(x^{\gamma_i}) \leftarrow -\frac{a_1}{m}(D_1^{(i)}(x_1))$.

4.2 Computing Minimal Element

We can obtain a minimal element with respect to $-v_P(\cdot)$ by extending the modification [7] of Paulus's LLL-like algorithm [10] in natural manner, since the fact of $b_i \equiv i \pmod{a_1}$ implies there exists an unique l such that $-v_P(f) = -v_P(f_l(x_1)x^{\gamma_l})$ for a nonzero element $f = \sum_{j=0}^{a_1-1} f_j(x_1)x^{\gamma_j}$.

Namely, for an ideal I, it is sufficient to find an basis (so-called reduced basis [10]) $\{f_0, \cdots, f_{a-1}\}$ such that $-v_P(f_i) \not\equiv -v_P(f_j) \bmod a_1$ $(0 \leq i < j \leq a-1)$. Then $f := \min_i\{-v_P(f_i)\}$ is the minimal element in I with respect to $-v_P(\cdot)$ [10].

And the complexity can be evaluated as follows:

Theorem 3 *[7] For a basis $\{f_0, \cdots, f_{a_1-1}\}$ of an ideal I, the minimal element is computed in*

$$O(a_1^2 s(a_1 s + \max_l\{b_l\}) \log^2 q),$$

if the degree of x_1 in $(f_{i,j})$ is bounded by s, where $f_i = (f_{i,0}, \cdots, f_{i,a_1-1})^t$ with $f_i = \sum_{j=0}^{a_1-1} f_{i,j}(x_1)x^{\gamma_j}$.

5 Complexity

In Section 4, we proposed a method for performing Jacobian group arithmetic on $C_{a_1,\cdots,a_t}$ curves (Algorithm 1).

And we can evaluate the complexity as follows: (Complexity of elementary operations is based on the facts in [7].)

Theorem 4 *For $C_{a_1,\cdots,a_t}$ curves, the Jacobian group arithmetic (Algorithm 1) is completed in*

$$O(a_1^{15} g^2 \log^2 q).$$

Remark 2 *Theorem 4 ensures that Jacobian group arithmetic on $C_{a_1,\cdots,a_t}$ curves is computed in $O(g^2)$ operations in the base field if the sizes of a_1 and q are bounded. And the assumption that the size of a_1 is bounded is natural, since a_1 is the minimal nonzero element in $\mathbf{A}_t$.*

References

[1] L.M.Adleman, J.DeMarrais and M.D.Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, ANTS-I, Algorithmic Number Theory (Lecture Notes in Computer Science, vol 877), 28-40, 1994.

[2] S. Arita, *Algorithms for Computations in Jacobian Group of C_{ab} Curve and Their Application to Discrete-Log Based Public Key Cryptosystems*, Conf. on The Mathematics of Public Key Cryptography, Toronto, 1999.

[3] S. Arita *Gaudry's Variant against C_{ab} curves*, Public Key Cryptography (Lecture Notes in Computer Science, vol 1751), 58-67, 2000.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, GTM 138, 1993.

[5] G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation **62** (1994), 865-874.

[6] P.Gaudry, *A variant of Adleman-DeMarris-Huang algorithm and its application to small genera*, Conf. on The Mathematics of Public Key Cryptography, Toronto, 1999.

[7] R.Harasawa, J.Suzuki, *Fast Jacobian Group Arithmetic on C_{ab} Curves*, in ANTS-4, Algorithmic Number Theory (Lecture Notes in Computer Science, vol 1838), 359-376, 2000.

[8] A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), 1639-1646.

[9] Shinji Miura, *Linear Codes on Affine Algebraic Cuves*, Trans. of IEICE, vol. J81-A, No. 10 (1998), pp. 1398-1421.

[10] S. Paulus, *Lattice basis reduction in function field* in ANTS-3, Algorithmic Number Theory(Lecture Notes in Computer Science, vol 1423), 567-575, 1998.

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1994.

[12] N. P. Smart, *On the performance of Hyperelliptic Cryptosystems*, Advances in Cryptology EUROCRYPTO'99 (Lecture Notes in Computer Science vol 1592), 165-175, 1998.

[13] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Springer-Verlag, 1993.

Appendix: The Degrees of Ideals

For $\forall f = \sum_{i=0}^{a_1-1} f_i(x_1)x^{\gamma_i} \in R$ ($\gamma_i \in T(A_t)$), we define $LM(f)$ as the maximal monomial in f with respect to $-v_P(\cdot)$, which is said to be a leading monomial of f.

And for a nonzero monomial $cx_1^d x^{\gamma_i}$ with $c \in K^*$ and $d \in \mathbf{N}_0$, we define $MD(cx_1^d x^{\gamma_i})$ as $MD(cx_1^d x^{\gamma_i}) = (d, 0, \cdots, 0) + \gamma_i \in \mathbf{N}_0^t$, which is said to be a multi-degree of $f_i(x_1)x^{\gamma_i}$.

Furthermore, for a nonzero ideal $I \subset R$, we define $\Delta(I)$ as follows:

$$\Delta(I) := \{\mathbf{M} \in \mathbf{N}_0^t | \ \mathbf{M} \notin MD(LM(I))\},$$

where $LM(I) := \{LM(f) | \ f \in I\}$ and $MD(0) := (\infty, \cdots, \infty)$.

Then, the following proposition is known:

Proposition 2 *[2]*

For the degree of an ideal $I \subset R$, it holds

$$\deg(I) = \#\Delta(I).$$

Then, we show the following proposition.

Proposition 3 *Let $I = \{f_0(x_1), \cdots, f_{a_1-1}(x_1)\}$ be the HNF representation of an ideal $I \subset R$, where $f_i(x_1) = (f_{i,0}(x_1), \cdots, f_{i,a_1-1}(x_1))^t$ for $f_i(x_1) = \sum_{j=0}^{a_1-1} f_{i,j}(x_1)x^{\gamma_j}$.*

Then,

$$\deg(I) = \deg_{x_1} \prod_i f_{i,i}(x_1) = \sum_i \deg_{x_1}(f_{i,i}(x_1)).$$

Proof of Proposition 3

Let $\{g_0(x_1), \cdots, g_{a_1-1}(x_1)\}$ be the reduced basis (Section 4-2 or [10]) of an ideal I. And we define $\Omega_i := \{LM(g_{i,\delta(i)}(x_1)x^{\gamma_{\delta(i)}}) \times (cx_1^d) | \ c \in K^*, \ d \in \mathbf{N}_0\}$.

Then, from $-v_P(g_i) \not\equiv -v_P(g_j) \bmod a_1$ $(0 \le i < j \le a-1)$,

$$\begin{cases} LM(I) = \cup_i \Omega_i \cup \{0\} \\ \Omega_i \cap \Omega_j = \phi \ (i \neq j), \end{cases}$$

where $\delta(i)$ satisfies $-v_P(g_i) = -v_P(g_{i,\delta(i)}(x_1)x^{\gamma_{\delta(i)}})$.

Therefore, it holds

$$\deg(I) = \#\Delta(I) = \sum_i \deg_{x_1} g_{i,\delta(i)}(x_1) = \deg_{x_1}(\det\{g_1(x_1), \cdots, g_t(x_1)\}).$$

And, since we obtain $\{g_0(x_1), \cdots, g_{a_1-1}(x_1)\}$ from $\{f_0(x_1), \cdots, f_{a_1-1}(x_1)\}$ by performing elementary operations on columns, the two determinants differ by some element in K^*.

Therefore,

$$\deg_{x_1}(\det\{g_0(x_1), \cdots, g_{a_1-1}(x_1)\}) = \deg_{x_1}(\prod_i f_{i,i}(x_1))$$

(note that $\{f_0(x_1), \cdots, f_{a_1-1}(x_1)\}$ is the HNF representation). **Q.E.D.**