AN ADDITION ALGORITHM ON THE JACOBIAN VARIETIES OF CURVES

(FOR APPLICATIONS TO PUBLIC KEY CRYPTOSYSTEM)

S. ARITA, S. MIURA, AND T. SEKIGUCHI*)

Abstract. The presented paper computes addition on Jacobian varieties of curves using its singular plane model. Given a nonsingular curve C, let C_1 be its singular (especially plane) C_A model. After making clear the relationship between generalized Jacobian variety of C_1 and Jacobian variety of C, we show that Arita's algorithm for non sigular C_A curves also works for generalized Jacobian variety of singular C_A curve C_1. This means that we can compute addition on Jacobian variety of any curve(with at least one rational point) using its singular C_A models.

1. Introduction

For a nonsingular curve C over a field k, the divisor class group $J(C)$ of degree zero is realized by the set of k-rational points of the Jacobian variety J_C of C. For a curve with only one singularity over a field k, the Jacobian variety is discussed by Serre [15], and it is called a generalized Jacobian variety. For such a singular curve, the set of k-rational points of the generalized Jacobian variety is realized also by divisor classes of degree zero, but it is much easier to express it as Picard group $\mathrm{Pic}^0(C)$ by using invertible sheaves of degree zero on C. Furthermore the concept of Picard group can be applicable to any singular curves.

Date: September 10, 2003.

*) This research was supported by Telecommunication Advancement Organization of Japan (TAO) and the Institute of Science and Engineering, Chuo University.

Throughout the paper, "Jacobi group" is referred to "Picard group" consisting of invertible sheaves of degree zero .

Now there are great concerns in addition algorithms on Jacobi groups of algebraic curves, stimulated by the success of elliptic curve cryptosystems. Besides elliptic curves, efficient addition algorithms on Jacobian groups of hyperelliptic, superelliptic, and (non singular) C_{ab} curves have been proposed.

The presented paper computes addition on Jacobian group of a curve using its singular plane model. Given a nonsingular curve C, let C_1 be its singular C_A model in the sense of Miura [13].

First, we make clear the relationship between the generalized Jacobian group of C_1 and the Jacobian group of C, and we see the generalized Jacobian group is naturally isomorphic to the ideal class group of the coordinate ring.

Next, we show that Arita's algorithm for ideal class group of Dedekind domain works in more general situation, and we see it computes addition on Jacobian group of singular C_A curve C_1.

These mean that we can compute addition on Jacobian group of any curve(with at least one rational point) using its singular C_A models.

In § 2, we see relations between generalized and ordinal Jacobian groups. In § 3 we review Miura's C_A model of a curve, and we discuss the Arita algorithm on coordinate ring of a singular curve in § 4. In the last section, we give some examples comparing the algorithms on Jacobian groups of a singular plane model and a non-singular model of a curve.

Throughout the paper, we will use the following notations:

- We mean simply by a curve a projective, absolutely integral curve.
- We mean by a semigroup a unitary commutative semigroup only.

· $\mathbb{N} := \{0, 1, 2, \dots\}$: the set of non-negative integers,
· p : a prime integer, and $q = p^e$ with $e > 0$,
· $k := \mathbb{F}_q$: the finite field consisting of q elements,
· C : a projective non-singular curve over k with k-rational point P,
· $K := k(C)$: the rational function field of C.

2. Jacobian groups of singular curves

Let C_0 be a singular curve over $k = \mathbb{F}_q$ with rational function field $K = k(C_0)$.

Hereafter we fix a k-rational point $\mathrm{P}_0 \in \mathrm{C}_0$. We suppose that P_0 is at most a cusp singularity of C_0, and let C_1 be the curve obtained by desingularizing only the singularity P_0. Note that if P_0 is a simple point, $C_1 = C_0$. We denote also by P_0 the point on C_1 lying over P_0 in C_0. Let $\pi : C \to C_1 \to C_0$ be the normalization of C_1 and so of C_0, and $g = g(C)$ be the genus of C.

2.1. Let $\mathcal{O} = \mathcal{O}_{C_1}$ be the structure sheaf of C_1. We denote by $\mathcal{K}$ the sheaf assigning K to each non-empty open subset of C_1. Then we have the exact sequence of sheaves on C_1:

$$0 \longrightarrow \mathcal{O}^* \longrightarrow \mathcal{K}^* \longrightarrow \mathcal{K}^*/\mathcal{O}^* \longrightarrow 0, \tag{1}$$

and we get a long exact sequence from this as follows:

$$0 \longrightarrow k^* \longrightarrow K^* \longrightarrow \mathrm{H}^0(C_1, \mathcal{K}^*/\mathcal{O}^*) \xrightarrow{\partial} \mathrm{H}^1(C_1, \mathcal{O}*) \longrightarrow 0.$$

The elements of $\mathrm{H}^0(C_1, \mathcal{K}^*/\mathcal{O}^*)$ are called the Cartier divisors on C_1, and the Cartier divisor class group is given by

$$\mathrm{CalCl}(C_1) := \mathrm{H}^0(C_1, \mathcal{K}^*/\mathcal{O}^*)/\mathrm{Image}(K^* \to \mathrm{H}^0(C_1, \mathcal{K}^*/\mathcal{O}^*)).$$

Moreover the Picard group is defined by

$$\mathrm{Pic}(C_1) := \mathrm{H}^1(C_1, \mathcal{O}^*) = \{\text{invertible sheaves on } C_1\}/\text{isomorphisms},$$

and we have the canonical isomorphism

$$\mathrm{Pic}(C_1) \cong \mathrm{CalCl}(C_1).$$

2.2. The normalization map $\pi : C \to C_1$ induces the exact sequence (cf. [6, Ch.II, Ex.6.9]):

$$0 \longrightarrow \oplus_{\mathrm{P}\in \mathrm{C}_1} \widetilde{\mathcal{O}}_{\mathrm{P}}^*/\mathcal{O}_{\mathrm{P}}^* \longrightarrow \mathrm{Pic}(C_1) \xrightarrow{\pi^*} \mathrm{Pic}(C) \longrightarrow 0, \tag{2}$$

where $\widetilde{\mathcal{O}}_{\mathrm{P}}$ means the integral closure of $\mathcal{O}_{\mathrm{P}}$ in K.

Example 2.1. *Suppose that a singular point* $\mathrm{P} \in \mathrm{C}_1$ *is* k*-rational. If* P *is an ordinary node and each point of* $\pi^{-1}(\mathrm{P})$ *is* k*-rational, then*

$$\widetilde{\mathcal{O}}_{\mathrm{P}}^*/\mathcal{O}_{\mathrm{P}}^* \cong \mathbb{G}_{m,k}.$$

If P *is an ordinary cusp, then*

$$\widetilde{\mathcal{O}}_{\mathrm{P}}^*/\mathcal{O}_{\mathrm{P}}^* \cong \mathbb{G}_{a,k}.$$

Remark. In general, for a singular point P, the group $\widetilde{\mathcal{O}}_{\mathrm{P}}^*/\mathcal{O}_{\mathrm{P}}^*$ is an extension of several torus, twisted torus or groups of Witt vectors (cf. [15]).

For a non-singular curve C, the groups $\mathrm{Pic}(C)$ and CalCl(C) are isomorphic to the divisor class group:

$$\mathrm{DivCl(C)} := \{k\text{-rational divisors on } C\}/\{(\mathrm{f}) \mid \mathrm{f} \in \mathrm{K}\}.$$

Hereafter we denote by $[D]$ the divisor class represented by a divisor D. We denote the subgroup consisting of divisors of degree 0 by

$$\mathrm{Pic}^0(C) \cong \mathrm{CalCl}^0(C) \cong \mathrm{DivCl}^0(C) \subset \mathrm{DivCl(C)},$$

and we put

$$\mathrm{Pic}^0(C_1) := (\pi^*)^{-1}(\mathrm{Pic}^0(C)) \subset \mathrm{Pic}(C_1). \tag{3}$$

Then the exact sequence (2) induces the exact one

$$\begin{aligned} 0 \longrightarrow \oplus_{\mathrm{P}\in \mathrm{C}_1} \widetilde{\mathcal{O}}^*_{\mathrm{P}}/\mathcal{O}^*_{\mathrm{P}} \longrightarrow \mathrm{Pic}^0(C_1) \\ \xrightarrow{\pi^*} \mathrm{Pic}^0(C) \longrightarrow 0. \end{aligned} \tag{4}$$

Hereafter we call $\mathrm{Pic}^0(C_1)$ the *Jacobian group* of C_1 as mentioned in the introduction.

2.3. We denote the coordinate ring of the affine scheme $C_0 \setminus \{\mathrm{P}_0\} = \mathrm{C}_1 \setminus \{\mathrm{P}_0\}$ by

$$R := \Gamma(C_0 \setminus \{\mathrm{P}_0\}, \mathcal{O}).$$

Let $\mathcal{I}(R)$ be the group of invertible fractional ideals of R, and $H(R)$ be the ideal class group:

$$\mathrm{H}(R) := \mathcal{I}(R)/\{(f) = fR \mid f \in K^*\}.$$

Since the invertible ideals are locally principal, we can easily see that each ideal $I \in \mathcal{I}(R)$ defines an invertible sheaf $\widetilde{I}$ on $\mathrm{SpecR} = \mathrm{C}_1 \setminus \{\mathrm{P}_0\}$. Conversely, since every coherent sheaf of modules on SpecR is given by $\widetilde{M}$ for an R-module M, each invertible sheaf L on SpecR is realized by $L = \widetilde{I}$ for an invertible ideal I of R. Therefore we have

$$\mathrm{H}(R) \cong \mathrm{Pic}(C_1 \setminus \{P_0\}).$$

By the similar exact sequence with (1) on $C_1 \setminus \{P_0\}$, we get the canonical isomorphism

$$\mathrm{CalCl}(\mathrm{C}_1 \setminus \{\mathrm{P}_0\}) \cong \mathrm{Pic}(\mathrm{C}_1 \setminus \{\mathrm{P}_0\}),$$

and we have

$$\mathrm{H}(R) \cong \mathrm{Pic}(C_1 \setminus \{P_0\}) \cong \mathrm{CalCl}(\mathrm{C}_1 \setminus \{\mathrm{P}_0\}). \tag{5}$$

2.4. Now, let $D = \{(f_{\mathrm{P}}, U_{\mathrm{P}})\}_{\mathrm{P}\in C_1\setminus\{P_0\}}$ be a Cartier divisor on $C_1 \setminus \{P_0\}$, where U_{P} is an affine open neighborhood at P in $C_1 \setminus \{P_0\}$ and $f_{\mathrm{P}} \in K$ with $f_{\mathrm{P}}/f_{\mathrm{Q}} \in \mathcal{O}(U_{\mathrm{P}} \cap U_{\mathrm{Q}})^*$ for any P, Q. We define the degree of D by

$$d(D) := \sum_{\mathrm{P}\in \mathrm{C}_1\setminus\{\mathrm{P}_0\}} \sum_{\mathrm{P}'\in\pi^{-1}(\mathrm{P})} \mathrm{ord}_{\mathrm{P}'}(\mathrm{f}_{\mathrm{P}}),$$

and an extended divisor on C_1 by

$$\widetilde{D} := D \cup \{(t^{-d(D)}, U_{\mathrm{P}_0})\},$$

where U_{P_1} is a sufficiently small affine open neighborhood at P_0 and t is a local parameter at P_0. Then obviously the correspondence $[D] \mapsto [\widetilde{D}]$ induces an isomorphism

$$\mathrm{CalCl}(\mathrm{C}_1 \setminus \{\mathrm{P}_0\}) \xrightarrow{\sim} \mathrm{CalCl}^0(C_1).$$

Therefore combining this with (5), we get an isomorphism

$$\mathrm{H}(R) \cong \mathrm{Pic}(C_1 \setminus \{P_0\}) \cong \mathrm{CalCl}(\mathrm{C}_1 \setminus \{\mathrm{P}_0\}) \cong \mathrm{CalCl}^0(\mathrm{C}_1) \cong \mathrm{Pic}^0(\mathrm{C}_1). \tag{6}$$

Notice that by the exact sequence (4) we can reduce the addition algorithm on $\mathrm{Pic}^0(C)$ to that on $\mathrm{Pic}^0(C_1)$, and the algorithm on $\mathrm{Pic}^0(C_1)$ is realized by the ideal class group on the ring $R = \Gamma(C_0 \setminus \{\mathrm{P}_0\}, \mathcal{O})$. Therefore, if we can take the model C_0 of K as a curve in a lower dimensional projective space (especially a plane) and we can choose the point P_0 in a nice way, the ring R can be expressed as the coordinate ring of an affine curve and we expect that the algorithm becomes much simpler.

Here we notice the following more or less well-known fact:

Lemma 2.1. *Let the ring R be as above. Then any invertible fractional ideal of R is generated by at most two elements. Moreover we can choose the generators of the ideal containing any chosen non-zero element of the ideal.*

Proof. Let I be an invertible fractional ideal of R. Then there exists a non-zero element $f \in K$ such that $fI \subset R$. Let $g \in fI$ be a non-zero element. By the primary decomposition, there exist finite number of maximal ideals $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_r$ such that

$$\sqrt{(g)} = \cap_1^r \mathfrak{M}_i.$$

Then we have

$$R/(g) \supset fI/(g) = \oplus_1^r fIR_{\mathfrak{M}_i}/gR_{\mathfrak{M}_i}.$$

Since fI is locally principal, there exist h_i such that $h_i R_{\mathfrak{M}_i} = fIR_{\mathfrak{M}_i}$ for each $i = 1, \ldots, r$. Let $h \in fI$ be an element such that $h \pmod{g} = (\overline{h}_1, \ldots, \overline{h}_r) \in \oplus_1^r fIR_{\mathfrak{M}_i}/gR_{\mathfrak{M}_i}$. Then we have $I = R(g/f) + R(h/f)$. ∎

Next we will explain how to get a nice model C_0 in a lower dimensional projective space (especially a plane) by using Miura's model, namely the C_A curves.

3. Miura's C_A curves

Here we will explain how to give a nice plane curve model for a given function field of one variable by using the Miura model of a curve (so-called C_A curve). The following is a review from Miura [13, Appendix], and one can refer the detail proofs to it.

3.1. We denote by $\mathbb{N}$ the semigroup consisting of non-negative integers. Let $M \subset \mathbb{N}$ be a subsemigroup of $\mathbb{N}$. Then M is finitely generated, that is to say, there exist $a_1, a_2, \ldots, a_t \in M$ with $a_1 < a_2 < \cdots < a_t$ such that

$$M =< a_1, a_2, \ldots, a_t >= \mathbb{N}a_1 + \mathbb{N}a_2 + \ldots + \mathbb{N}a_t$$

with $t \leq a_1$. For a system of generators $A = \{a_1, \ldots, a_t\}$ of M, we can see that the complement of M in $\mathbb{N}$ is finite if and only if

$(a_1, a_2, \dots, a_t) = 1$, and in this case, more precisely we have

$$\#(\mathbb{N} \setminus M) = \sum_{i=1}^{a_1-1} \left[\frac{b_i}{a_1} \right],$$

where

$$b_i := \mathrm{Min}\{a \in M \mid a \equiv i \pmod{a_1}\} \tag{7}$$

for each $i = 0, 1, \dots, a_1 - 1$. In this case, we call M a *numerical semigroup*.

3.2. Hereafter let M be a numerical semigroup with a system of generators $A = \{a_1, a_2, \dots, a_t\}$ with $t \leq a_1$.

Associating with this numerical semigroup M, we define a surjective map

$$\Psi : \mathbb{N}^t \to M$$

by

$$\Psi(n_1, n_2, \dots, n_t) := \sum_{i=1}^{t} n_i a_i.$$

By using this map, we can define a monomial order on $\mathbb{N}^t$ as follows.

Definition 3.1. *For tow elements* $\boldsymbol{m} = (m_1, m_2, \dots, m_t)$ *and* $\boldsymbol{n} = (n_1, n_2, \dots, n_t)$ *of* $\mathbb{N}^t$*, we define*

$$\boldsymbol{m} < \boldsymbol{n} \overset{\text{def}}{\iff} \begin{cases} \Psi(\boldsymbol{m}) < \Psi(\boldsymbol{n}) \\ \textit{or} \\ \Psi(\boldsymbol{m}) = \Psi(\boldsymbol{n}) \ \textit{and} \ m_1 = n_1, \dots, m_i = n_i, m_{i+1} > n_{i+1}. \end{cases}$$

Then this gives a monomial order on $\mathbb{N}^t$*, that is to say, any non-empty subset of* $\mathbb{N}^t$ *has a smallest element, and if* $\boldsymbol{a} < \boldsymbol{b}$ *then* $\boldsymbol{a} + \boldsymbol{c} < \boldsymbol{b} + \boldsymbol{c}$ *for any element* $\boldsymbol{c} \in \mathbb{N}^t$*. We call this order the* C_A-order *on* $\mathbb{N}^t$*.*

Next we define some subsets of $\mathbb{N}^t$ for later use.

Definition 3.2.

$$B(A) := \{\boldsymbol{m}(a) \mid a \in M\} \subset \mathbb{N}^t,$$

$$T(A) := \{\boldsymbol{m}(b_i) \in B(A) \mid i = 0, 1, \dots, a_1 - 1\},$$

$$V(A) := \left\{ \boldsymbol{\ell} \in \mathbb{N}^t \setminus B(A) \;\middle|\; \begin{array}{l} \textit{if } \boldsymbol{\ell} = \boldsymbol{m} + \boldsymbol{n} \\ \textit{with } \boldsymbol{m} \in \mathbb{N}^t \setminus B(A) \textit{ and } \boldsymbol{n} \in \mathbb{N}^t, \\ \textit{then } \boldsymbol{n} = \boldsymbol{0} \end{array} \right\},$$

where for $a \in M$,

$$\boldsymbol{m}(a) := \mathrm{Min}\{\boldsymbol{n} \mid \boldsymbol{n} \in \Psi^{-1}(a)\},$$

and b_i*'s are the numbers given by (7).*

Then we can see that $V(A)$ is a finite set and

$$B(A) = T(A) + \mathbb{N} \times \{0\}^{t-1}.$$

3.3. Under the notations in 3.2, we consider the polynomials $F_{\boldsymbol{m}}$ ($\boldsymbol{m} \in V(A)$) in $k[X] = k[X_1, X_2, \dots, X_t]$ satisfying the following conditions.

(D1) For each $\boldsymbol{m} \in V(A)$,

$$F_{\boldsymbol{m}} = X^{\boldsymbol{m}} + a_{\boldsymbol{\ell}} X^{\boldsymbol{\ell}} + \sum_{\boldsymbol{n}} a_{\boldsymbol{n}} X^{\boldsymbol{n}},$$

where $\boldsymbol{\ell} = \boldsymbol{m}(\Psi(\boldsymbol{m}))$, $a_{\boldsymbol{\ell}} \neq 0$, and the summation runs over $\boldsymbol{n} \in B(A)$ with $\boldsymbol{n} < \boldsymbol{m}$. Here for $\boldsymbol{m} = (m_1, m_2, \dots, m_t)$, we understand that $X^{\boldsymbol{m}} = \prod_{i=1}^{t} X_i^{m_i}$.

(D2) $\left(\sum_{\boldsymbol{n} \in B(A)} k X^{\boldsymbol{n}}\right) \cap (F_{\boldsymbol{m}} \mid \boldsymbol{m} \in V(A)) = (0)$

3.4. Next we start with a non-singular model C of a function field K of one variable over k. Let $\mathrm{P} \in C$ be a k-rational point. We put

$$L(\infty \mathrm{P}) := \cup_{n \geq 0} L(n\mathrm{P}) \subset \mathrm{K},$$

and

$$M(\mathrm{P}) := \{-\mathrm{ord}_{\mathrm{P}}(f) \mid f \in L(\infty \mathrm{P}) \setminus \{0\}\} \subset \mathbb{N}.$$

Then $M(\mathrm{P})$ is a numerical semigroup.

Here we take a subalgebra R of $L(\infty \mathrm{P})$ such that $k \subset R \subset L(\infty \mathrm{P})$, and define a semigroup by

$$M(R) := \{-\mathrm{ord}_{\mathrm{P}}(f) \mid f \in R \setminus \{0\}\} \subset \mathbb{N}.$$

Let $A = \{a_1, a_2, \ldots, a_t\}$ be a system of generators of $M(R)$.Then we have the following easy fact.

Lemma 3.1. *The filed of fractions* $\mathrm{f.f.(R)}$ *of* R *coincides with* K *if and only if* $(a_1, a_2, \ldots, a_t) = 1$.

Hereafter we suppose that $\mathrm{f.f.(R)} = \mathrm{K}$, that is to say, $M(R)$ is a numerical semigroup. For this semigroup $M(R)$, we adopt the above notations. We choose function $f_i \in R$ such that $\mathrm{ord_P(f_i)} = -\mathrm{a_i}$ for each $i = 1, 2, \ldots, t$ and we consider the surjection

$$\Theta : k[X] = k[X_1, X_2, \ldots, X_t] \to R$$

defined by $\Theta(F) := F(f_1, f_2, \ldots, f_t)$ for $F \in k[X]$. Then the kernel $I(R) := \mathrm{Ker}(\Theta)$ is generated by the polynomials satisfying the conditions (D1) and (D2). Miura showed the converse was also true. Eventually he showed the following.

Theorem 3.2. (Miura) *Let* M *be a numerical semigroup with a system of generators* $A = \{a_1, a_2, \ldots, a_t\}$. *Then an ideal* I *of* $k[X] = k[X_1, X_2, \ldots, X_t]$ *is generated by polynomials satisfying (D1) and (D2) if and only if there exist a function field* K *of one variable over* k *and a* k*-rational point* P *of the non-singular model* C *of* K *and a subalgebra* $k \subset R \subset L(\infty \mathrm{P})$ *such that* $\mathrm{f.f.(R)} = \mathrm{K}$ *and* $I = I(R)$. *In this case, the polynomials satisfying (D1) and (D2) form a Gröbner basis of* I, *and the projective model* $C_0(A)$ *of* $\mathrm{Spec(k[X]/I)} \subset \mathbb{A}^{\mathrm{t}}_{\mathrm{k}}$ *in* $\mathbb{P}^t_k$ *has only one*

infinity point P*, and which is at most a cuspidal singularity. Moreover, the affine model* Spec(k[X]/I) *of* K *is non-singular if and only if* $R = L(\infty \mathrm{P})$.

Definition 3.3. *Under the notations of Theorem 3.2, when the ideal* $I = I(R) \subset k[X]$ *is corresponding to a numerical semigroup* M *with system of generators* $A = \{a_1, a_2, \ldots, a_t\}$*, we call* Spec(k[X]/I(R)) *or* $C_0(A)$ *a* C_A-curve *of* K*. For a numerical semigroup* M *generated by* A*, if there exists an affine non-singular* C_A-curve*,* M *is called a* Weierstrass numerical semigroup.

By using the Riemann-Roch theorem for any curve (cf. [15, IV]), we obtain the genus formula as follows.

Proposition 3.3. *Let* C' *be the curve given by desingularizing only the infinity point of a* C_A*-curve* $C_0(A)$*. Then the arithmetic genus* $g_a(C') := \dim \mathrm{H}^1(C', \mathcal{O}_{C'})$ *is given by*

$$g_a(C') = \#(\mathbb{N} \setminus M) = \sum_{i=1}^{a_1 - 1} \left[\frac{b_i}{a_1} \right],$$

where b_i*'s are given by (7). In particular, when* M *has two generators, that is to say,* $A = \{a, b\}$ *with* $(a, b) = 1$*, we have*

$$g_a(C') = \frac{(a-1)(b-1)}{2}.$$

In the sequel, our algorithm is based on Theorem 3.2. We must note that in this case of M having two generators, we do not need to consider the condition (D2) in the theorem, because if we take a polynomial satisfying the condition (D1), then the condition (D2) is automatically satisfied. Let M be a numerical semigroup with generators $A = \{a, b\}$ with $(a, b) = 1$. For $i = 0, 1, \ldots, a - 1$, we set

$$b_i := \mathrm{Min}\{\alpha \in M \mid \alpha \equiv i \pmod{a}\},$$

as above. Then

$$T(A) = \{\boldsymbol{m}(b_i) \mid i = 0, 1, \ldots, a-1\} = \{(0, i) \mid i = 0, 1, \ldots, a-1\},$$
$$B(A) = T(A) + \mathbb{N} \times \{0\} \subset \mathbb{N}^2,$$

and

$$V(A) = \{(0, a)\}.$$

Therefore in this case, Theorem 3.2 can be rewritten as follows.

Corollary 3.4. *Let a, b be positive integers with $(a, b) = 1$. Let*

$$F(X, Y) := Y^a + \alpha_0 X^b + \sum_{ia+jb<ab} \alpha_{ij} X^i Y^j,$$

with $\alpha_0, \alpha_{ij} \in k$ and $\alpha_0 \neq 0$, that is to say, $F(X, Y)$ is a polynomial satisfying the condition (D1). Put $R = k[X, Y]/(F)$ and $K = \mathrm{f.f.(R)}$. Then SpecR *is a C_{ab}-curve with arithmetic genus*

$$g_a = \frac{(a-1)(b-1)}{2}.$$

Conversely let K be a function field of one variable over k, and C be the non-singular model of K. Let $\mathrm{P} \in C$ be a k-rational point. We choose two functions $f, g \in L(\infty \mathrm{P}) \subset K$ with coprime orders $a := -\mathrm{ord_P}(f)$ and $b := -\mathrm{ord_P}(g)$. Then the relation $F(X, Y) \in k[X, Y]$ of f, g satisfies the condition (D1) and automatically (D2), and the C_{ab}-curve Spec(k[X, Y]/(F)) *gives the affine plane model of K.*

Example 3.1. *Let*

$$F(X, Y) := Y^2 - X^3 \quad \textit{and} \quad G(X, Y) := Y^2 - X^3 - X^2.$$

Then these satisfy the condition (D1) for $A = \{2, 3\}$, and these are cuspidal and nodal $C_{2,3}$-curves of rational function field $k(t)$ respectively.

The inclusions

$$\begin{array}{rcl} R := k[X,Y]/(F) & \hookrightarrow & k[t]; \\ \overline{X} & \mapsto & t^2 \\ \overline{Y} & \mapsto & t^3 \end{array} \qquad \begin{array}{rcl} R' := k[X,Y]/(G) & \hookrightarrow & k[t] \\ \overline{X} & \mapsto & t^2-1 \\ \overline{Y} & \mapsto & t(t^2-1) \end{array}$$

define the normalizations. The ideal class group $\mathrm{H}(R)$ *is given as follows.*

$$\mathrm{H}(R) = \{\wp_a \mid a \in k \setminus \{0\}\} \cup \{[(1)]\},$$

where

$$\wp_a = [(X - a^2, Y - aX)] = \{f \cdot (X - a^2, Y - aX) \mid f \in \text{f.f.R}\}.$$

The group law is given by

$$\wp_a \cdot \wp_b = \begin{cases} \wp_{ab/(a+b)} & \text{if } a+b \neq 0 \\ [(1)] & \text{if } a+b = 0. \end{cases}$$

Therefore we have an isomorphism

$$\begin{array}{rcl} \mathrm{H}(R) & \to & \mathbb{G}_a(k) = k. \\ \wp_a & \mapsto & 1/a \\ [(1)] & \mapsto & 0 \end{array}$$

Similarly, we have

$$\mathrm{H}(R') = \{\wp_a \mid a \in k \setminus \{\pm 1\}\} \cup \{[(1)]\},$$

where

$$\wp_a = [(X - a^2 + 1, Y - aX)] = \{f \cdot (X - a^2 + 1, Y - aX) \mid f \in \text{f.f.R}\}.$$

The group law is given by

$$\wp_a \cdot \wp_b = \begin{cases} \wp_{(1+ab)/(a+b)} & \text{if } a+b \neq 0 \\ [(1)] & \text{if } a+b = 0, \end{cases}$$

and an isomorphism

$$\begin{aligned} \mathrm{H}(R') &\to \mathbb{G}_m(k) = k^*. \\ \wp_a &\mapsto (a-1)/(a+1) \\ [(1)] &\mapsto 1 \end{aligned}$$

Remark. Maclachlam [9] showed that any numerical semigroup generated by 3 elements containing 3 is Weierstrass, and later Pinkham [14] and Waldi [16] showed independently that every numerical semigroup generated by 3 elements is Weierstrass.

Example 3.2. *Let* $A = \{3, 5, 7\}$. *Then we have*

$$\begin{aligned} T(3,5,7) &= \{(0,0,0), (0,0,1), (0,1,0)\} \\ B(3,5,7) &= \{(i,0,0), (i,0,1), (i,1,0) \mid i = 0, 1, \dots\} \\ V(3,5,7) &= \{(0,2,0), (0,1,1), (0,0,2)\} \end{aligned}$$

and $\boldsymbol{m}(\Psi(0,2,0)) = \boldsymbol{m}(10) = (1,0,1)$, $\boldsymbol{m}(\Psi(0,1,1)) = \boldsymbol{m}(12) = (4,0,0)$ *and* $\boldsymbol{m}(\Psi(0,0,2)) = \boldsymbol{m}(14) = (3,1,0)$. *Therefore the general forms of the polynomials satisfying (D1) are given by the following equations:*

$$\begin{aligned} F_1(X,Y,Z) &= Y^2 + \alpha_0 XZ + \alpha_1 X^3 + \alpha_2 XY + \alpha_3 Z + \alpha_4 X^2 \\ &\quad + \alpha_5 Y + \alpha_7 X + \alpha_{10} \\ F_2(X,Y,Z) &= YZ + \beta_0 X^4 + \beta_1 X^2 Y + \beta_2 XZ + \beta_3 X^3 + \beta_4 XY \\ &\quad + \beta_5 Z + \beta_6 X^2 + \beta_7 Y + \beta_9 X + \beta_{12} \\ F_3(X,Y,Z) &= Z^2 + \gamma_0 X^3 Y + \gamma_1 X^2 Z + \gamma_2 X^4 + \gamma_3 X^2 Y + \gamma_4 XZ \\ &\quad + \gamma_5 X^3 + \gamma_6 XY + \gamma_7 Z + \gamma_8 X^2 + \gamma_9 Y + \gamma_{11} X + \gamma_{14}, \end{aligned}$$

where $\alpha_i, \beta_j, \gamma_k \in k$ *and* $\alpha_0\beta_0\gamma_0 \neq 0$. *By the above remark, suitable equations* F_1, F_2, F_3 *define a non-singular* $C_{3,5,7}$*-curve* C. *Moreover, eliminating the variable* Z *from* $F_1(X,Y,Z)$ *and* $F_2(X,Y,Z)$, *we can*

obtain an equation

$$G(X,Y) = Y^3 + \delta_0 X^5 + \delta_1 X^3 Y + \delta_2 XY^2 + \delta_3 X^4 + \delta_4 X^2 Y + \delta_5 Y^2 + \delta_6 X^3 + \delta_7 XY + \delta_9 X^2 + \delta_{10} Y + \delta_{12} X + \delta_{15},$$

which gives the $C_{3,5}$-model C_0 of this curve C. In this case, $g_a(C) = g(C) = 3$ and $g_a(C_0) = 4$.

4. Arita algorithm on generalized Jacobian group of singular C_A curve

In the last section, we see the generalized Jacobian group of singular C_A curve is isomorphic to the ideal class group of the coordinate ring. This section gives an addition algorithm on the generalized Jacobian group as a multiplication algorithm in the ideal class group.

As the notation of Theorem 3.2, let

$K :=$ a function field of one variable over a field k,
$\mathrm{P} :=$ a k-rational place of K, namely, $\mathcal{O}_{\mathrm{P}}/\mathfrak{M}_{\mathrm{P}} = k$,
$R :=$ a k-subalgebra of $L(\infty \mathrm{P})$ with $K = \mathrm{f.f.R}$,
$M(R) =< A >$ with $A = \{a_1, a_2, \ldots, a_t\}$,
$I = I(R) = \mathrm{Ker}(\Theta : k[X] = k[X_1, X_2, \ldots, X_t] \to R)$,
$C_A := \mathrm{SpecR} = \mathrm{Spec(k[X]/I)} \subset \mathbb{A}^{\mathrm{t}}_{\mathrm{k}}$.

Note that we can choose any numerical subsemigroup of $M(\mathrm{P})$ as $M(R)$, and in that case, C_A is nonsingular if and only if $M(R) = M(P)$, namely $R = L(\infty \mathrm{P})$. Moreover note that $k[X]$ has the C_A-order which is monomial, and we can consider Gröbner basis for any ideal of $k[X]$, and $I = I(R)$ is given by a Gröbner basis. Hereafter, for an ideal $\mathfrak{a} \subset R$, we put $\mathfrak{A} = \Theta^{-1}(\mathfrak{a}) \subset k[X] = k[X_1, X_2, \ldots, X_t]$.

For an invertible ideal $\mathfrak{a}$ of R, let

$$h \in 1 :_K \mathfrak{a} = \mathfrak{a}^{-1}$$

be a non-zero element of $\mathfrak{a}^{-1}$ with smallest minus order $-\mathrm{ord}_{\mathrm{P}}(h)$.

Then we define $\mathfrak{a}^*$ by

$$\mathfrak{a}^* := h \cdot \mathfrak{a}.$$

Obviously the fractional ideal $\mathfrak{a}^*$ is contained in R. To specify a special representative of an ideal class $[\mathfrak{a}]$, we adopt the ideal $\mathfrak{a}^*$. In fact, we can see the following fact.

Lemma 4.1. *The ideal $\mathfrak{a}^*$ is uniquely determined depending only on the ideal class $[\mathfrak{a}]$.*

Sublemma 4.2. *For an invertible ideal $\mathfrak{a}$ of R, a non-zero element h of $\mathfrak{a}$ with smallest minus order $-\mathrm{ord_P(h)}$ is unique up to constant multiplication.*

Proof. Let h an h' be non-zero elements of $\mathfrak{a}$ with smallest minus order $-\mathrm{ord_P}(h') = -\mathrm{ord_P}(h) =: n$. Then there exists a constant element $c \in k$ such that $-\mathrm{ord_P}(h' - ch) < n$. Since $h' - ch \in \mathfrak{a}$, we get $h' - ch = 0$. ■

Proof of the lemma. Let $\mathfrak{a}' \in [\mathfrak{a}]$, and $h' \in (\mathfrak{a}')^{-1}$ be a non-zero element with smallest minus order $-\mathrm{ord_P}(h')$. Let $(\mathfrak{a}')^* = h' \cdot \mathfrak{a}'$. By the assumption, there exists an element $u \in K$ such that $\mathfrak{a}' = u \cdot \mathfrak{a}$. Now let $h \in \mathfrak{a}^{-1}$ be a non-zero element with smallest minus order $-\mathrm{ord_P}(h)$. Then since $h' \in (\mathfrak{a}')^{-1} = u^{-1}\mathfrak{a}^{-1}$, we have $h' = h/u$ up to constant. Therefore we have $(\mathfrak{a}')^* = h' \cdot \mathfrak{a}' = (h/u) \cdot u \cdot \mathfrak{a} = h \cdot \mathfrak{a} = \mathfrak{a}^*$. ■

We call $\mathfrak{a}^* = h \cdot \mathfrak{a}$ (or $\mathfrak{A}^* := \Theta^{-1}(\mathfrak{a}^*) \subset k[X] = k[X_1, X_2, \ldots, X_t]$) the *reduced ideal* of $\mathfrak{a}$. An essential point of the algorithm of ideal classes is how to compute the reduced ideal $\mathfrak{a}^*$ or equivalently the rational function h. In the sequel, we calculate a rational function h as a fraction of elements of R or $k[X]$. In fact, we take a non-zero element $f \in \mathfrak{a}$ and let

$$g \in (f) :_K \mathfrak{a} = (f) :_R \mathfrak{a} = f \cdot \mathfrak{a}^{-1}$$

be a non-zero element of $f \cdot \mathfrak{a}^{-1}$ with smallest minus order $-\mathrm{ord}_{\mathrm{P}}(g)$. Then $h = g/f$. In this case, we see that

$$\Theta^{-1}(f \cdot \mathfrak{a}^{-1}) = (fk[X] + I) :_{k[X]} \mathfrak{A}.$$

Using reduced ideals as a representative system of ideal classes, we get the following addition algorithm on generalized Jacobian group of a singular C_A curve.

Algorithm 1 (Addition in generalized Jacobian group of C_A curve)**.** *Inputs: generators of invertible ideals* $\mathfrak{a}_1$, $\mathfrak{a}_2$ *contained in the coordinate ring* R
Output: Gröbner basis of reduced ideal $(\mathfrak{a}_1\mathfrak{a}_1)^*$

(1) *take generators* $(f_1, f_2, \dots, f_\ell) + I = \mathfrak{A}_1$, $(g_1, g_2, \dots, g_m) + I = \mathfrak{A}_2$
(2) *take a non-zero element* $f \in \mathfrak{A}_1\mathfrak{A}_2 \setminus I$
(3) *take* $g \in \big((fk[X] + I) :_{k[X]} \mathfrak{A}_1\mathfrak{A}_2\big)$ *with smallest* C_A*-order*
(4) *Gröbner basis of* $(\mathfrak{A}_1\mathfrak{A}_2)^* = h \cdot (\mathfrak{A}_1\mathfrak{A}_2)$, *where* $h = g/f$

5. An example

Let k be a prime field of characteristic $p = 83$. We take a singular C_{35} curve C defined over k by

$$\begin{aligned} &-30 - 11X - 6Y - 6X^2 - 31XY - 80X^3 \\ &\quad - 59Y^2 - 35X^2Y - 41X^4 - 7XY^2 - 78X^3Y - 10X^5 + Y^3. \end{aligned}$$

C has the unique singular point (70,65). Let G be the maximal ideal $(X - 2, Y - 33)$ of R. Since G corresponds to a nonsingular point, G is invertible.

The normalization $\tilde{C}$ of C is defined by

$$64 + 4X + 30X^2 + 30X^3 + 76Y + 75XY + Y^2 + 52Z + 4XZ,$$

$$10 + 27X + 16X^2 + 6X^3 + 44X^4 + 69Y$$
$$+ 16XY + 27X^2Y + 31Z + XZ + YZ,$$

$$22 + 32X + 77X^2 + 30X^3 + 11X^4 + 17Y$$
$$+ 25XY + 3X^2Y + 72X^3Y + 45Z + 32XZ + 76X^2Z + Z^2.$$

G is the projected point of $G_0 = (2, 33, -21)$ on $\tilde{C}$.

G_0 has the order $n = 2^3 \cdot 3 \cdot 7 \cdot 11$ in Jacobian group of $\tilde{C}$. So, $n \cdot G$ must be killed by the $p - 1$ multiplication in the generalized Jacobian group of C. In fact, using a sample program in the appendix we see that

$$H = n \cdot G$$
$$= (Y^2 + 14Y + 34X + 38, XY + 13Y + 18X + 68, X^2 + 26X + 3)$$

and

$$(p - 1) \cdot H = (1).$$

Note the zero set of H is $\{(70, 4), (70, 65)\} \subset C$.

References

[1] S. Arita, *Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log-based public key cryptosystems*, Conference on The Mathematics of Public Key Cryptography, Toronto, 1999

[2] S. Arita, *The discretes-log-based public key cryptosystems using algebraic curves of heigher degree*, in Japanese, Doctor Thethis (Chuo University), 2000

[3] D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Mathematics of Computation, 48(177), 95–101(1987)

[4] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, 31, 469–472(1985)

[5] S. D. Galbraith, S. Paulus and N. P. Smart, *Arithmetic on superelliptic curves*, J. Cryptology 12, 193–196(1999)

[6] R. Hartshore, *Aalgebraic geometry*, Springer-Verlag, 1977

[7] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation, 48, 203–209(1987)

[8] N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptoography 1, 139–150(1989)

[9] C. Maclachlam, *Weierstrass points on compact Riemann surfaces*, J. London Math. Soc. (2) 3, 722–724(1971)

[10] **Magma**, `URL http://www.maths.usyd.edu.au:8000/u/magma/.`

[11] R. Matsumoto and S. Miura, *Finding a basis of a linear system with pairwise distinct discrete valuations on an algebaraic curve*, J. Symbolic Computation 30, 309–323(2000)

[12] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology-Crypto'85(LNCS 218), 417–426(1986)

[13] S. Miura, *The linear code on affine algebraic curves*, in Japanese, Shingakuron(A), vol. J81-A, No. 10, 1398–1421(1998)

[14] H. C. Pinkham, *Deformations of algebraic varieties with* $\mathbb{G}_m$ *action*, Astérisque 20, 1–131(1974)

[15] J.-P. Serre, *Groupes algébriquees et corps de classes*, Hermann, Paris(1961)

[16] R. Waldi, *Zur Konstruktion von Weierstrasspunkten mit vorgegebener Halbgruppe*, Manuscripta Math. 30, 257–278(1980)

Appendix A. Sample codes

Here, we show sample codes of Algorithm 1 in Magma V2.7-2[10]. Loading "singularC35.mag", you can verify computations in section 5. Try

```
jPower(n,G);
```

which computes n multiple of G in the singular C_{35} curve C. By loading "C357.mag", you can compute the same multiple in the normalization $\tilde{C}$ which is a C_{357} curve.

cabkernel.mag.

```
// Addition in Jacobian group


jCompose := function(I, J)
```

```
    K := I*J+P;
    Groebner(K);
    return K;
end function;

MinimumNonZeroFnc := function(I)
    i := #Basis(I);
    while i gt 0 do
        f := Basis(I)[i];
        if NormalForm(f, P) ne 0
            then return f;
        end if;
        i := i - 1;
    end while;
    return 0; // error
end function;

jReduce := function(I)
    f := MinimumNonZeroFnc(I);
    J := ideal<R | f> + P;
    Groebner(J);
    J := IdealQuotient(J,I) + P;
    Groebner(J);
    return J;
end function;

jSum := function(I,J)
    K := jCompose(I,J);
    K := jReduce(K);
    K := jReduce(K);
    return K;
end function;
```

```
jPower := function(n, I)
    r := ideal<R | 1>; // zero element
    e := I;
    i := n;
    while  i gt 0  do
        if (i mod 2) eq 1 then
            r := jSum(r, e);
            i := (i-1) div 2;
        else
            i := i div 2;
        end if;
        if i gt 0 then
            e := jSum(e, e);
        end if;
    end while;
    return r;
end function;
```

singularC35.mag.

```
p := 83;
k := FiniteField(p);

R<X,Y> := PolynomialRing(k,2,"weight",
    [3,5, 0,1]);
f := -30 - 11*X - 6*Y - 6*X^2 - 31*X*Y - 80*X^3 -
    59*Y^2 - 35*X^2*Y - 41*X^4 - 7*X*Y^2 - 78*X^3*Y - 10*X^5 + Y^3;
P := ideal< R | f >;
// unique singular point (-13,-18)
SI := P + ideal<R | Derivative(f,1), Derivative(f,2)>;
G := ideal< R | X-2,Y-33>;
```

```
n := 2^3*3*7*11; // order of G0
load "cabkernel.mag";
```

c357.mag.

```
p := 83;
k := FiniteField(p);

R<X,Y,Z> := PolynomialRing(k,3,"weight",
    [3,5,7,
     0,1,1,
     0,0,1]);
P := ideal< R | 64 + 4*X + 30*X^2 + 30*X^3 + 76*Y + 75*X*Y + Y^2 + 52*Z + 4*X*Z,
    10 + 27*X + 16*X^2 + 6*X^3 + 44*X^4 + 69*Y + 16*X*Y + 27*X^2*Y + 31*Z +
        X*Z + Y*Z,
    22 + 32*X + 77*X^2 + 30*X^3 + 11*X^4 + 17*Y + 25*X*Y + 3*X^2*Y + 72*X^3*Y +
        45*Z + 32*X*Z + 76*X^2*Z + Z^2>;
G := ideal< R | X-2,Y-33, Z+21>;
n := 2^3*3*7*11;
load "cabkernel.mag";
```

(Seigo Arita) NEC Corporation 4-1-1 Miyazaki, Miyamae-ku, Kawasaki-shi, Kanagawa-ken 216- Japan

E-mail address: arita@ccm.cl.nec.co.jp

(Shinji Miura) 2-48-11 Eifuku, Suginami-ku, Tokyo 168-0064 Japan

E-mail address: miura-1003-luna@docomo.ne.jp

(Tsutomu Sekiguchi) Department of Mathematics, Faculty of Science and Engeneering, Chuo University 1-13-27 Kasuga Bunkyo-ku Tokyo 112-8551, Japan

E-mail address: sekiguti@math.chuo-u.ac.jp