中央大学理工学研究所論文集　第17号　2011年
Journal of the Institute of Science and Engineering. Chuo University

GEOMETRIC ASPECTS OF THE ADDITION ALGORITHM ON THE PICARD GROUP OF A C_{ab} CURVE

SHINJI MIURA AND TSUTOMU SEKIGUCHI*)

Abstract. In the previous paper [3], we proposed to use the Picard group of the plane model, which is so-called C_{ab} model admitting singularities, of a curve of any genus for realizing a faster addition algorithm on the Jacobian group of the curve. In the paper, we present the explicit addition algorithm on the Picard group of a C_{ab} curve from the geometric view point, which will give a generalization of Cantor's algorithm on the Jacobian group of a hyperelliptic curves and a supplement of the argument given in [4].

1. Introduction

Throughout the paper, we denote by p a prime integer, and k a finite field $\mathbb{F}_q$ of $q = p^e$ elements. Moreover, we denote by K a one-dimentional function field over k of genus g. Let C be a C_{ab} affine plane model (cf. §2 for details) of K (in general, it has some singularities), and $\overline{C}$ be the projective closure of C. Then $\overline{C} \setminus C$ consists of one point P_∞, which is at most cusp singularity of $\overline{C}$. We denote by $\overline{C}^*$ the curve obtained by desingularizing $\overline{C}$ only at the point P_∞. Moreover let $\pi : \widetilde{C} \to \overline{C}^*$ be the normalization of $\overline{C}^*$. Then the Jacobian group $J(\widetilde{C})$ of $\widetilde{C}$ is nothing but the Picard group $\mathrm{Pic}^0(\widetilde{C})$, and as is explaned in the previous paper [3], we have the canonical isomorphism

$$\mathrm{Pic}(C) \cong \mathrm{Pic}^0(\overline{C}^*)$$

and an exact sequence

$$0 \longrightarrow H \longrightarrow \mathrm{Pic}(C) \cong \mathrm{Pic}^0(\overline{C}^*) \xrightarrow{\pi^*} \mathrm{Pic}^0(\widetilde{C}) \longrightarrow 0,$$

Date: January 27, 2012.
*) This research was supported by Research and Development Institute Chuo University.

where H is the group consisting of k-rational points of the affine group scheme appearing as the singularities of C. Note that H is negligible for application to cryptography. Therefore we devote ourselves to consider the addition algorithm on $\mathrm{Pic}^0(C)$ instead of on $\mathrm{Pic}(\widetilde{C})$.

The Picard group $\mathrm{Pic}(C)$ is nothing but the ideal class group of the coordinate ring $R = \Gamma(C, \mathcal{O}_C)$ of C, and for giving explicitly the addition algorithm on $\mathrm{Pic}(C)$, we need to settle the following three problems:

(1) To give the best way for representing a given ideal of R by which we can insist easily a computer to recognize it.
(2) To give the explicit multiplication algorithm of ideals of R.
(3) To give an efficient algorithm for fixing the special representative (so-called **reduced ideal**) of a given ideal class of R.

An explicit algorithm of these items for any non-singular C_A curves was given first by Arita [1, 2] by using Gröbner bases. But the algorithm of Gröbner bases is rather heavy. For the coordinate ring of any C_A curve, even it has some singularities, any invertible ideal is generated by two elements, and for an affine C_{ab} curve, it would be very easy to decide the two generators of any invertible ideal, and to write the algorithm of the above items by using such generators of the ideals as discussed by [4]. In fact, by [4], Basiri, Enge, Faugère and Gürel give a precise algorithm for the above items for most of ideals, but not all ideals, for non-singular cubic curves. In the paper, we give algorithms of the above items for any invertible ideals without any exceptions for any affine C_{ab} curves by using suitable two generators of the ideals.

In §2, we give a review of Miura's affine C_{ab} plane model of a curve, and next §3, in the coordinate ring R, we discuss the generators of invertible ideals and the multiplications of invertible ideals. In §4, we give an algorithm of the reduced representative of an ideal class of R.

2. Review of Miura's C_{ab} model of a curve

We will recall here the method how to give an affine model of a curve, which is called Miura's C_{ab} model of a curve, from [3].

Under the notations in Introduction, let $\wp$ be a fixed k-rational place of K, and v be the corresponding valuation of K. We define the subring $L(\infty\wp)$ of K by

$$L(\infty\wp) := \{f \in K \mid \wp'(f) \neq \infty \quad \text{for any place } \wp' \neq \wp\}.$$

We choose two functions $f, g \in L(\infty\wp)$ with $v(f) = -a$, $v(g) = -b$, $0 < a < b$ and $(a, b) = 1$. Then the k-algebra $R = k[f, g]$ generated by f, g gives an affine plane model $C = \mathrm{Spec}R$ of K, that is to say, $K = \mathrm{f.f.}R$ (the filed of fractions of R). This kind of models of a curve have been studied deeply by S. Miura mainly for constructing the algebraic geometric code theory. We call C an affine plane $\boldsymbol{C_{ab}}$ **model** of K, and the projective closure $\overline{C} \subset \mathbb{P}^2_k$ of C a projective plane $\boldsymbol{C_{ab}}$ **model** of K. As in Introduction, $\overline{C} \setminus C$ consits of only one point P_∞ corresponding to $\wp$. Let $\overline{C}^*$ be the curve obtained by desingularizing $\overline{C}$ only at the point P_∞, and

$$\varphi : k[X, Y] \to R$$

be the k-algebra homomorphim defined by $\varphi(X) = f$ and $\varphi(Y) = g$. We define the so-called $\boldsymbol{C_{ab}}$ **order** $\boldsymbol{\Psi}$ on $k[X, Y]$ by $\Psi(X^\ell Y^m) := \ell a + mb$. Then the relation of f, g is given by a polynomial F of type

$$F(X, Y) = Y^a + \sum_{\ell a + mb < ab} a_{\ell,m} X^\ell Y^m + X^b,$$

and $\mathrm{Ker}\Psi = (F) \subset k[X, Y]$. Namely we have

$$R \cong k[X, Y]/(F).$$

Hereafter, we identify R with $k[X, Y]/(F)$. The arithmetic genus g_a of $\overline{C}^*$ is given by

$$g_a = \dim \mathrm{H}^1(\overline{C}^*, \mathcal{O}_{\overline{C}^*}) = \frac{(a-1)(b-1)}{2}.$$

For later use, we introduce the following notations.

Let

$$\left.\begin{aligned} u(X, Y) &= u_0(X)Y^\ell + u_1(X)Y^{\ell-1} + \ldots + u_\ell(X) \\ v(X, Y) &= v_0(X)Y^m + v_1(X)Y^{m-1} + \ldots + v_m(X) \end{aligned}\right\} \in k[X, Y].$$

We define the content of u in Y by

$$\mathrm{cont}_Y(u) := (u_0(X), u_1(X), \dots, u_\ell(X)) \in k[X].$$

We denote by $\boldsymbol{(u,v)_Y}$ the polynomial in X obtained by eliminating the variable Y from u and v. Moreover, we denote by $R_Y(u,v)$ the resultant of u an v:

$$R_Y(u,v) = \begin{vmatrix} u_0 & u_1 & \cdots & u_\ell & & & \\ & u_0 & u_1 & \cdots & u_\ell & & \\ & & \ddots & \ddots & \cdots & \ddots & \\ u_0 & u_1 & \cdots & u_\ell & & & \\ & v_0 & v_1 & \cdots & v_m & & \\ & & \ddots & \ddots & \cdots & \ddots & \\ & & & v_0 & v_1 & \cdots & v_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \\ \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} \ell \end{matrix} \in k[X].$$

Let $u(X,Y) = u_0(X)\prod_{i=1}^{\ell}(Y-\alpha_i)$ be the factorization of $u(X,Y)$ as a polynomial in Y over an algebraic closure of the rational function field $k(X)$. Then the following is a well-known formula:

$$R_Y(u,v) = u_0^m \prod_{i=1}^{\ell} v(X,\alpha_i). \tag{1}$$

3. Representation of ideals

3.1. As in the previous section, $C = \mathrm{Spec}R$ with $R = k[X,Y]/(F(X,Y))$ is a C_{ab} affine model of K and we use the same notations. Hereafter, we consider C as the covering $C = \mathrm{Spec}R \to \mathrm{Spec}k[X]$. Let $\overline{k}$ be an algebraic closure of k, $\overline{R} = R \otimes_k \overline{k}$, and $C^{\mathrm{geom}} = C \times_{\mathrm{Spec}k} \mathrm{Spec}\overline{k} = \mathrm{Spec}\overline{R}$. Next we will start our argument by the following well-known fact.

Lemma 3.1. *Let $\mathfrak{a}$ be a non-principal invertible ideal in R. For any chosen non-zero element u of $\mathfrak{a}$, there exists an element $v \in \mathfrak{a}$ such that $\mathfrak{a} = (u,v)$.*

(e.g. cf.[3, Lemma 2.1])

As is well-known also, any ideal in R is characterised locally by the following fact.

Lemma 3.2. *Let R be an integral domain. Then for any ideal $\mathfrak{a}$ of R, we have*

$$\mathfrak{a} = \cap_{\mathfrak{m}} \mathfrak{a} R_{\mathfrak{m}},$$

where the intersection is taken in the field of fractions of R, and $\mathfrak{m}$ runs over all maximal ideals of R.

Next is a direct consequence of this lemma.

Corollary 3.3. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in R. If $R_{\mathfrak{m}}\mathfrak{a} = R_{\mathfrak{m}}\mathfrak{b}$ for any maximal ideals $\mathfrak{m}$ of R, then $\mathfrak{a} = \mathfrak{b}$.*

Hereafter, we denote by $\mathfrak{a}_{\mathfrak{m}}$ the localized ideal $R_{\mathfrak{m}}\mathfrak{a}$.

3.2.

Definition 3.1. *For an invertivle ideal $\mathfrak{a}$ of R, we put $\overline{V}(\mathfrak{a}) = \mathrm{Spec}(\overline{R}/\mathfrak{a}) \subset C^{\mathrm{geom}}$. When the support of $\overline{V}(\mathfrak{a})$ is $\mathrm{Sup}(\overline{V}(\mathfrak{a})) = \{\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_r\}$, we denote the set of X-coordinates of P_i's by $X(\mathfrak{a}) := \{X(\mathrm{P}_1), X(\mathrm{P}_2), \ldots, X(\mathrm{P}_r)\}$. For a point $\mathrm{P} \in C^{\mathrm{geom}}$, we define the multiplicity $m_{\mathrm{P}}(\mathfrak{a})$ by*

$$m_{\mathrm{P}}(\mathfrak{a}) := \dim_k \left(R_{\mathrm{P}}/\mathfrak{a}R_{\mathrm{P}}\right).$$

For a non-singular point $\mathrm{P} \in C^{\mathrm{geom}}$, we define a number $n_{\mathrm{P}}(\mathfrak{a})$ by

$$n_{\mathrm{P}}(\mathfrak{a}) := \begin{cases} m_{\mathrm{P}}(\mathfrak{a}) & \text{if } C/\mathrm{Spec}k[X] \text{ ramifies at } P \\ 1 & \text{otherwise.} \end{cases}$$

For $\alpha \in X(\mathfrak{a})$ with no singular point in $\overline{V}(\mathfrak{a}) \cap \overline{V}(X - \alpha)$, we put

$$n(\alpha) = n(\alpha; \mathfrak{a}) := \sum_{1}^{r} n_{\mathrm{P}_i}(\mathfrak{a}),$$

and $n(\mathfrak{a}) := \mathrm{Max}\{n(\alpha) \mid \alpha \in X(\mathfrak{a})\}$. Note that if none of points of $\overline{V}(\mathfrak{a}) \cap \overline{V}(X - \alpha)$ is a ramification point over $\mathrm{Spec}\overline{k}[X]$, then

$$n(\alpha) = \sharp\left(\mathrm{Sup}\left(\overline{V}(\mathfrak{a})\right) \cap \mathrm{Sup}\left(\overline{V}(X - \alpha)\right)\right).$$

For a point $\mathrm{P} \in \mathrm{Sup}(\overline{V}(\mathfrak{a}))$ with $X(\mathrm{P}) = \alpha$, we define the number $e(\mathfrak{a} : \mathrm{P})$ by

$$e(\mathrm{P}; \mathfrak{a}) = \text{ the smallest positive integer } e \text{ such that } (X - \alpha)^e \in \mathfrak{a}\overline{R}_{\mathrm{P}}.$$

When $\mathfrak{a}R_{\mathrm{P}} = (f_{\mathrm{P}})$, *we can easily see the following:*

$$e(\mathrm{P};\mathfrak{a}) = \begin{cases} v_{\mathrm{P}}(f_{\mathrm{P}}) = I(V(\mathfrak{a}) \cap C;\mathrm{P}) & \text{if } P \text{ is not a ramification point} \\ & \text{of } C^{\mathrm{geom}}/\mathrm{Spec}\overline{k}[X], \\ \left\lceil \frac{I(V(\mathfrak{a})\cap C;\mathrm{P})}{I(V(X-a)\cap C;\mathrm{P})} \right\rceil & \text{if } P \text{ is a ramification simple} \\ & \text{point of } C, \end{cases}$$

where $I(A \cap B;\mathrm{P})$ *is the intersection number at* P *of curves* A *and* B.

For $\alpha \in X(\mathfrak{a})$, *we set*

$$e(\alpha;\mathfrak{a}) := \mathrm{Max}\left\{e(\mathrm{P};\mathfrak{a}) \mid \mathrm{P} \in \mathrm{Sup}(\overline{V}(\mathfrak{a})) \cap \mathrm{Sup}(\overline{V}(X-\alpha))\right\},$$

and

$$e(\mathfrak{a}) := \mathrm{Max}\left\{e(\alpha;\mathfrak{a}) \mid \alpha \in X(\mathfrak{a})\right\}.$$

Then we can easily see the equality:

$$(u,F)_Y = \prod_{\alpha \in X(u)} (X-\alpha)^{e(\alpha;u)},$$

for a polynomial $u(X,Y)$.

For any invertible ideal $\mathfrak{a}$ in R, we put

$$\mathfrak{a}_* := \mathfrak{a} \cap k[X].$$

Lemma 3.4. *Let*

$$u(X,Y) = u_0(X)Y^{\ell} + u_1(X)Y^{\ell-1} + \cdots + u_{\ell}(X) \quad \in R,$$

with $1 \leq \ell \leq a-1$. *Then the ideal* $(u)_* = (u) \cap k[X]$ *is given by*

$$(u)_* = \left(\mathrm{Nm}_{k(X)(u)/k(X)}(u)\right) = \left((u,F)_Y\right),$$

where $\mathrm{Nm}_{k(X)(u)/k(X)}$ *means the norm of the extension* $k(X)(u)/k(X)$. *In particular, if* a *is a prime number, then by noting* (1), *we have*

$$(u)_* = (R_Y(F,u)).$$

Next is easy from a geometric viewpoint.

Lemma 3.5. *For an invertible ideal* $\mathfrak{a}$ *in* R, *we have*

$$\mathfrak{a}_* = \prod_{a \in X(\mathfrak{a})} (X-a)^{e(\mathfrak{a};a)}.$$

Lemma 3.6. *Let $\mathfrak{a} = (u, v)$ be a non-principal ideal of R with $1 \leq \deg_Y u$, $\deg_Y v \leq a-1$. Let $f(X) := (u, v)_Y$. We choose $c \in k\backslash\{0\}$ so that the ideal $(f^2, cu-v)$ contains u. The probability of choosing such c is at least $(q - (\deg f)a)/q$. Then we have*

$$\mathfrak{a} = (f, cu - v).$$

Proof. We choose a constant c so that for any point $\mathrm{P} \in \overline{V}(f)$, if $u(\mathrm{P}) \neq 0$ then $cu(\mathrm{P}) - v(\mathrm{P}) \neq 0$, and if $u(\mathrm{P}) = 0$ and $v(\mathrm{P}) = 0$ then $\mathfrak{a}R_{\mathrm{P}} = (cu - v)$. Therefore ovbiously $\overline{V}(\mathfrak{a}) = \overline{V}((f, cu - v))$, and for any point $\mathrm{P} \in \overline{V}(\mathfrak{a})$, $\mathfrak{a}R_{\mathrm{P}} = (cu - v)$. Therefore we have our assertion. □

Definition 3.2. *If a pair of generators $(f(X), u(X, Y))$ of an invertible ideal $\mathfrak{a}$ satisfies that $\mathfrak{a}_* = (f)$ and $\mathfrak{a} = (f^2, u)$, we call the pair of generaters $(f(X), u(X, Y))$ a* **P-basis** *of $\mathfrak{a}$. The second condition of a P-basis is nothing but that u is a local generator of the ideal $\mathfrak{a}$ at each point.*

For a given non-principal ideal, a P-basis can be given in the following way.

Proposition 3.7. *Let $\mathfrak{a} = (u, v)$ be a non-principal ideal of R with $1 \leq \deg_Y u$, $\deg_Y v \leq a-1$. Now we choose $c \in k\backslash\{0\}$ so that for $\mathrm{P} \in \overline{V}((u, F)_Y)$, if $u(\mathrm{P}) \neq 0$ then $cf(\mathrm{P}) \neq u(\mathrm{P})$, and if $u(\mathrm{P}) = 0$ and $v(\mathrm{P}) = 0$ then $\mathfrak{a}R_{\mathrm{P}} = (cu - v)$. This condition on c is checked by the above lemma. When we put $h(X) := ((u, F)_Y, (cu - v, F)_Y)$, then we have*

$$\mathfrak{a}_* = (h), \quad \textit{and} \quad \mathfrak{a} = (h, cu - v).$$

Proof. . By Lemma 3.5, we have

$$\mathfrak{a}_* = \prod_{\alpha \in X(\mathfrak{a})} (X - \alpha)^{e(\alpha;\mathfrak{a})}.$$

On the other hand, obviously $f(X) := (u, F)_Y$ and $g(X) := (cu - v, F)_Y$ are contained in $\mathfrak{a}_*$, and $f(X) = 0$ (resp. $g(X) = 0$) gives all X-coordinates of the points of $\overline{V}(u)$ (resp. of the points of $\overline{V}(cu - v)$); that is to say, $f(X) = g(X) = 0$ gives the whole X-coordinates of the points $\mathrm{P} \in \overline{V}(\mathfrak{a})$.

Therefor, we have

$$((u,F)_Y,(cu-v,F)_Y)=\prod_{\alpha\in X(\mathfrak{a})}(X-\alpha)^{\mathrm{Min}\{e(\mathrm{P};u),e(\mathrm{P};cu-v)\}}.$$

By our choice of c, we have

$$\begin{aligned}e(\alpha;\mathfrak{a})&=\mathrm{Max}_{\mathrm{P}\in\overline{V}(X-\alpha)}\{\mathrm{Min}\{e(\mathrm{P};u),e(\mathrm{P};cu-v)\}\}\\&=\mathrm{Max}_{\mathrm{P}\in\overline{V}(X-\alpha)}\{e(\mathrm{P};cu-v)\}\end{aligned}$$

(since $e(\mathrm{P};u)\geq e(\mathrm{P};cu-v)$ for any $\mathrm{P}\in\overline{V}(X-\alpha)$,)

$$\begin{aligned}&=\mathrm{Min}\left\{\mathrm{Max}_{\mathrm{P}\in\overline{V}(X-\alpha)}\{e(\mathrm{P};u)\},\mathrm{Max}_{\mathrm{P}\in\overline{V}(X-\alpha)}\{e(\mathrm{P};cu-v)\}\right\}\\&=\mathrm{Min}\{e(\alpha;u),e(\alpha;cu-v)\},\end{aligned}$$

and we get $\mathfrak{a}_*=(h)$. Moreover, by our choice of c, $\mathrm{Sup}\left(\overline{V}(h,cu-v)\right)=\mathrm{Sup}(\overline{V}(\mathfrak{a}))$ and $\mathfrak{a}=(h,cu-v)$. The condition on the constant c is equivalent to that $V(\mathfrak{a})=V(u,cu-v)$ and $\mathfrak{a}_{\mathrm{P}}=(cu-v)$ at each point $\mathrm{P}\in V(\mathfrak{a})$. Therefore this condition on c is equivalent to $\mathfrak{a}=(u^2,cu-v)$ since $V(\mathfrak{a})=V(u^2,cu-v)$. □

Proposition 3.8. *Let $\mathfrak{a}=(f(X),v(X,Y))$ be an invertible ideal in R. Then we have $\mathfrak{a}_*=(f(X),(v,F)_Y)$.*

3.3. We can easily see the following.

Lemma 3.9. *Let $\mathfrak{a}=(f(X),v(X,Y))$ be an ideal of R. If $f(X)=f_1(X)f_2(X)$ with $(f_1,f_2)=1$, then $\mathfrak{a}=(f_1,v)(f_2,v)$.*

Conversely we have the following.

Proposition 3.10. *Let $\mathfrak{a}_i=(f_i(X),u_i(X,Y))$ $(i=1,2)$ be invertible ideals of R with monic polynmials u_i in Y:*

$$u_i=Y^{\ell_i}+u_{i1}(X)Y^{\ell_i-1}+\cdots+u_{i\ell_i}(X)\qquad(i=1,2).$$

Suppose that $1 \leq \ell_1 \leq \ell_2$. *We assume that* $(f_1(X), f_2(X)) = 1$. *Then when we take* $\alpha_i(X,Y) \in k[X,Y]$ $(i = 1,2)$ *such that* $\overline{V}(\alpha_i, f_i) = \emptyset$, *we have*

$$\mathfrak{a}_1\mathfrak{a}_2 = (f_1 f_2, \alpha_2 f_1 u_2 + \alpha_1 f_2 u_1).$$

In particular, we take polynomials $c(x), d(x) \in k[X]$ *such that* $c(X)f_1(X) + d(X)f_2(X) = 1$. *Furthermore, let* $\beta \in k$ *be an element such that* $\overline{V}((f_1(X), Y^{\ell_2-\ell_1} - \beta)) = \emptyset$. *Then we have*

$$\mathfrak{a}_1\mathfrak{a}_2 = (f_1(X)f_2(X), u(X,Y)),$$

where $u(X,Y)$ *is the monic polynomial in* Y *defined by*

$$u(X,Y) = c(X)f_1(X)u_2(X) + d(X)f_2(X)(Y^{\ell_2-\ell_1} - \beta)u_1(X).$$

Proof. Since, by our assumption, at each point of $\overline{V}(f_1(X))$, $\alpha_1 f_2$ is invertible, and also at each point of $\overline{V}(f_2(X))$, $\alpha_2 f_1$ is invertible, we have our requiring equation. □

Lemma 3.11. *Let* $\mathfrak{a} \subset R$ *be an invertible non-principal ideal with no singular point in* $\overline{V}(\mathfrak{a})$. *Suppose that* $\mathfrak{a}_* = (f(X)^e)$ *with irreducible monic polynomial* $f(X) \in k[X]$ *and* $e \geq 1$. *Then* $\mathfrak{a} = (f(X)^e, u(X,Y))$, *with*

$$u(X,Y) = Y^{n(\mathfrak{a})} + u_1(X)Y^{n(\mathfrak{a})-1} + \cdots + u_{n(\mathfrak{a})}(X).$$

In this case, if $\overline{V}(\mathfrak{a})$ *has no ramification points, and* $v(X,Y) \in \mathfrak{a}$ *and* $1 \leq \deg_Y v(X,Y) = e < n(\mathfrak{a})$, *then* $v(X,Y)$ *is divisible by* $f(X)$,

Proof. Let $\mathfrak{a} = (f(X)^e, v(X,Y))$, $\alpha \in \overline{k}$ be a solution of $f(X) = 0$, and σ be the Frobenius automorphism of $\overline{k}/k$ defined by $x^\sigma = x^q$ for any $x \in \overline{k}$. Then

$$f(X) = \prod_{i=0}^{d-1}(X - \alpha^{\sigma^i}),$$

where $d = \deg f$. By Lemma 3.9

$$\overline{\mathfrak{a}} := \mathfrak{a}\overline{R} = \prod_{i=0}^{d-1} \mathfrak{a}_0^{\sigma^i}$$

with

$$\mathfrak{a}_0 := ((X-\alpha)^e, v) \subset \overline{R}.$$

For each point $\mathrm{P} \in \overline{V}(X-\alpha) \cap \overline{V}(\mathfrak{a})$, if P is not a ramification point over $\mathrm{Spec}\overline{k}[X]$, there exists a polynomial $f_{\mathrm{P}}(X)$ such that $I(\overline{V}(Y - f_{\mathrm{P}}(X)) \cap C^{\mathrm{alg}}; \mathrm{P}) = m_{\mathrm{P}}(\mathfrak{a})$, and in this case we put $u_{\mathrm{P}}(X,Y) = Y - f_{\mathrm{P}}(X)$. If P is a ramification point, then we put $u_{\mathrm{P}}(X,Y) := (Y - Y(\mathrm{P}))^{m_{\mathrm{P}}(\mathfrak{a})}$. We define

$$u_\alpha(X,Y) := \prod_{\mathrm{P}} u_{\mathrm{P}}(X,Y),$$

where P runs over $\overline{V}(X-\alpha) \cap \overline{V}(\mathfrak{a})$,

$$f_i(X) := f(X)/(X - \alpha^{\sigma^i}) \quad \text{for each } 0 \le i \le d-1,$$

and

$$u(X,Y) := \sum_{i=0}^{d-1} f_i(X)^e u_\alpha^{\sigma^i}(X,Y).$$

Then obviously we have

$$\mathfrak{a}_0 = \left((X-\alpha)^e, u_\alpha(X,Y)\right),$$

and by Prop. 3.10

$$\overline{\mathfrak{a}} = \prod_{i=0}^{d-1} \mathfrak{a}_0^{\sigma^i} = \left(f(X)^e, u(X,Y)\right).$$

Since $f(X) \in k[X]$ and $u(X,Y) \in k[X,Y]$, we have

$$\mathfrak{a} = \left(f(X)^e, u(X,Y)\right).$$

Here obviously the degrees in Y of $u_\alpha(X,Y)$ and of $u(X,Y)$ are $n(\mathfrak{a})$, and the coefficient of $Y^{n(\mathfrak{a})}$ is $\sum_{i=1}^{d-1} (f_\alpha^\sigma(X))^e$, which we denote by $\ell(X)$. Since $\ell(X)$ is coprime to $f(X)^e$, there exist polynomials $g(X), h(X) \in k[X]$ such that $g(X)f(X)^e + h(X)\ell(X) = 1$. Then $\mathfrak{a} = (f(X)^e, h(X)u(X,Y))$, and $h(X)u(X,Y)$ is equivalent to a monic polynomial in Y modulo $f(X)^e$.

Moreover if $\overline{V}(\mathfrak{a})$ has no ramification points, then $n(\mathfrak{a})$ is the number $\sharp\left(\overline{V}(X-\alpha) \cap \overline{V}(\mathfrak{a})\right)$. Therefore for $v(X,Y) \in \mathfrak{a}$ if $\deg_Y v(X,Y) < n(\mathfrak{a})$, since $v(\alpha,Y) = 0$ has zeros of number $n(\mathfrak{a})$, we have $v(\alpha,Y) = 0$. Therefore we have $(X-\alpha)|v(X,Y)$ and $f(X)|v(X,Y)$. □

Proposition 3.12. *Let* $\mathfrak{a} = (f(X), u(X,Y)) \subset R$ *be an invertible non-principal ideal. Then we can choose, in probavility of at least* $q/\sharp\overline{V}(\mathfrak{a})$*, a constant* $c \in k$ *satisfying the condition:*

$$(1) \qquad \mathfrak{a}_{\mathrm{P}} = (u(X,Y) + cf(X)) \quad \textit{for each point} \quad \mathrm{P} \in \overline{V}(\mathfrak{a}).$$

Moreover, the condition (1) is equivalent to each of the following conditions:

$$(2) \qquad f(X) \in (f(X)^2, u(X,Y) + cf(X)).$$

$$(3) \qquad \mathfrak{a} = (f(X)^2, u(X,Y) + cf(X)).$$

Proof. In fact, at each point $\mathrm{P} \in \overline{V}(\mathfrak{a})$, $\mathfrak{a}_{\mathrm{P}}$ is generated by $f(X)$ or $u(X,Y)$. Therefore we can choose a constant $c \in k$ so that it is generated by $u(X,Y)+cf(X)$. Moreover, if (2) is satisfied, then $\mathfrak{a} = (f(X)^2, u(X,Y) + cf(X))$ and the condition (1) is obvious. Conversely, if (1) is satisfied, then since $V(\mathfrak{a}) = V((f(X)^2, u(X,Y) + cf(X))$, we have the equality $\mathfrak{a} = (f(X)^2, u(X,Y) + cf(X))$. □

Proposition 3.13. *Let* $\mathfrak{a}_1 = (f_1(X), v_1(X,Y)), \mathfrak{a}_2 = (f_2(X), v_2(X,Y))$ *be invertible ideals in* R*. Assume that* $\sqrt{(f_1)} = \sqrt{(f_2)}$ *and for each point* $\mathrm{P} \in V(\mathfrak{a}_i)$*,* $\mathfrak{a}_{i\mathrm{P}} = (v_i(X,Y))$ *for* $i = 1, 2$*. Then we have*

$$\mathfrak{a}_1\mathfrak{a}_2 = (f_1(X)f_2(X), v_1(X,Y)v_2(X,Y)).$$

In fact, since $V(\mathfrak{a}_1\mathfrak{a}_2) = V(f_1(X)f_2(X), v_1(X,Y)v_2(X,Y))$, we have our assertion.

The following is useful to make an algorithm of computing a power of ideals.

Proposition 3.14. *For an ivertible ideal* $\mathfrak{a} = (f(X), u(X,Y))$*, we have*

$$\mathfrak{a}^n = (f(X)^n, u(X,Y)^n)$$

for any positive integer n*,*

Summarlizing above arguments, we obtain the following.

Theorem 3.15. *Let* $\mathfrak{a}_i = (f_i(X), v_i(X,Y))$ $(i = 1,2)$ *be invertible ideals with monic polynomials* v_i *in* Y. *Suppose that* $m = \deg_Y v_1 \geq n = \deg_Y v_2$. *For each* $i = 1,2$, *we set* $f_i = f_{i1}(X)f_{i2}(X)$ *so that*

$$(f_{i1}, f_{i2}) = 1 \quad \textit{and} \quad \sqrt{(f_1, f_2)} = \sqrt{(f_{12})} = \sqrt{(f_{22})}.$$

Let $a_1(X), a_2(X)$ *and* $b_1(X), b_2(X)$ *be the polynomials such that*

$$a_1 f_{11} + a_2 f_{21} = 1 \quad \textit{and} \quad b_1 f_{11} f_{21} + b_2 f_{12} f_{22} = 1.$$

We choose $\alpha, \beta, c_1, c_2 \in k$ *so that for any* $(\gamma_1, \gamma_2) \in \overline{V}(f_{21}, F)$, $\gamma_2^{m-n} \neq \alpha$; *for any* $(\delta_1, \delta_2) \in \overline{V}(f_{11}f_{22}, F)$, $\delta_2^n \neq \beta$; *and for each* $i = 1,2$ *and any* $P \in V(f_{i2}, v_2)$, $(f_{i2}, v_i)_{\mathrm{P}} = (v_i + c_i f_{i2})$. *We put*

$$u := a_2 f_{21}(Y^{m-n} - \alpha)v_1 + a_1 f_{11} v_2,$$
$$w := b_2 f_{12} f_{22}(Y^n - \beta)u + b_1 f_{11} f_{21}(v_1 + c_1 f_{12})(v_2 + c_2 f_{22}).$$

Then we have

$$\mathfrak{a}_1 \mathfrak{a}_2 = (f_1 f_2, w).$$

Remark. Note that the generators of type $f(X)$ and $u(X,Y)$ for an invertible ideal $\mathfrak{a}$ are not unique for $\mathfrak{a}$, and if we want to recognize an invertible ideal uniquely, we need to take the Gröbner basis of it.

4. Reduced Ideal

To establish an addition algorithm of ideal classes, we must specify a special element uniquely for a given ideal class, which we call the reduced ideal for the ideal class. Here we recall the definition of the reduced ideal for an invertible ideal.

Let $\mathfrak{a}$ be an invertible ideal in R, and let

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

be a non-zero element of $\mathfrak{a}^{-1}$ with smallest minus order $-\mathrm{ord}_{\mathrm{P}}(h)$. Here we mean by $\mathfrak{a} :_K \mathfrak{b}$ for ivertible ideals $\mathfrak{a}$, $\mathfrak{b}$ the fractional ideal $(\mathfrak{a} :_K \mathfrak{b}) := \{f \in K \mid f\mathfrak{b} \subset \mathfrak{a}\}$. Then we define the reduced ideal $\mathfrak{a}^*$ of $\mathfrak{a}$ by

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

Note that the reduced ideal $\mathfrak{a}^*$ is uniquely determined for the ideal class $[\mathfrak{a}]$ represented by $\mathfrak{a}$ (cf. [3, Lem. 4.1].)

For an invertible ideal $\mathfrak{a} = (f(X), u(X,Y))$ in $R = k[X,Y]/(F(X,Y))$, its reduced ideal $\mathfrak{a}^*$ is given explicitly as in [3] in the following way:

> Take an element $h \in ((f) : \mathfrak{a})$ with smallest Ψ-order $\Psi(h)$. Next take the element $g \in R$ such that $hu = fg$. Then we have $\mathfrak{a}^* = (h, g)$.

For the invertible ideal $\mathfrak{a} = (f(X), u(X,Y))$, the reduced ideal $\mathfrak{a}^* = (h,g)$ are given by the following algorithm:

$$\begin{aligned} e &:= \Psi(f), \\ h &:= \sum_{\substack{0 \le j \le a-1,\, 0 \le i \\ ai+bj \le e-1}} b_{ij} X^i Y^j, \end{aligned}$$

dividing hu by F as polynomials in Y

$$\begin{aligned} hu &\equiv \sum_{0 \le \ell \le a-1} P_\ell(X) Y^\ell \pmod{F}, \\ R_\ell(X) &:\equiv P_\ell(X) \pmod{f}. \end{aligned}$$

Then the coefficients of $R_\ell(X)$'s are linear combinations of b_{ij}'s, and we solve the equations in b_{ij}'s so that h has the smallest Ψ-order:

$$R_\ell(X) = 0 \quad \text{for } 0 \le \ell \le a-1,$$

and we set

$$g := \sum_{0 \le \ell \le a-1} \left(P_\ell(X)/f(X)\right) Y^\ell.$$

If solutions are $b_{ij} = 0$ only, then we set

$$h = f(X) \quad \text{and} \quad g = u.$$

5. Explicit algorithms

As before, let $F(X,Y)$ be a C_{ab} curve and $R = k[X,Y]/F$ be the coordinate ring of the affine model.

5.1. Algorithm $L\mathfrak{a}$**.** Let $\mathfrak{a} = (u, v)$ $(u = u(X, Y),\ v = v(X, Y))$ be an invertible ideal in R. Next is an algorithm to give the generators of lexicographic order of $\mathfrak{a}$ starting from u, v.

Algorithm $L\mathfrak{a}$

1. $L\mathfrak{a} := \mathfrak{a}$
2. $f(X) := (u^2, F)_Y$
3. $v_o := v$
4.

$$\ell(X, Y) := \ell_0(X)Y^{a-1} + \ell_1(X)Y^{a-2} + \ldots + \ell_a(X) \quad (\deg \ell_i(X) \leq \deg f(X) - 1)$$
$$m(X, Y) := m_0(X)Y^{a-1} + m_1(X)Y^{a^2} + \ldots + m_a(X) \quad (\deg m_i(X) \leq \deg f(X) - 1)$$

5. while $u \equiv \ell u^2 + m v_0 \pmod{(F, f)}$ has no roots ℓ, m, do
6. random number $c \in k$
7. $v_0 := cu - v_0$
8. $h := ((u, F)_Y, (v_0, F)_Y)$
9. $L\mathfrak{a} := (h, v_0)$

5.2. Algorithm $R\mathfrak{a}$**.** Let $\mathfrak{a} = (f(X), u(X, Y))$ be an invertible ideal.

Algorithm $R\mathfrak{a}$

1. $R\mathfrak{a} := \mathfrak{a}$
2. $e := \Psi(f)$
3. $h := \displaystyle\sum_{\substack{0 \leq j \leq a-1 \\ 0 \leq i \\ ai+bj \leq e-1}} b_{ij} X^i Y^j$
4. $\displaystyle\sum_{0 \leq \ell \leq a-1} P_i(X) Y^\ell := hu \pmod{F}$
5. $R_i(X) := P_i(X) \pmod{f}$
6. If there is a non-tribial solution of the equations in b_{ij}'s:

$$R_i(X) = 0 \quad \text{for} \quad 0 \leq i \leq a - 1,$$

we choose the solution b_{ij}^o's so that h has the smallest Ψ-order.

7.

$$g := \sum_{0 \le \ell \le a-1} (P_\ell(X)/f(X))\, Y^\ell,$$

$$h := h \quad \text{with replaced } b_{ij}\text{'s by } b_{ij}^o\text{'s}$$

8. $R\mathfrak{a} := L(h, g)$

9. else

$$R\mathfrak{a} := \mathfrak{a}$$

5.3. Algorithm $M(\mathfrak{a} \cdot \mathfrak{b})$.

Algorithm $M_0(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$

Let $\mathfrak{a}_1 = (f_1(X), u_1(X, Y))$, $\mathfrak{a}_2 = (f_2(X), u_2(X, Y))$ be invertible ideals where u_i's are monic polynomials in Y. Assume $(f_1, f_2) = 1$.

1. $M_0 f := f_1 f_2$

$M_0 u := 1$

$M_0(\mathfrak{a}_1 \cdot \mathfrak{a}_2) := (M_0 f, M_0 u)$

$\ell_1 := \deg_Y u_1$

$\ell_2 := \deg_Y u_2$

2. choose $a(X)$, $b(X)$ such that

$$a(X) f_1(X) + b(X) f_2(X) = 1$$

3. if $\ell_1 = \ell_2$,

$$M_0 u := b(X) f_2(X) u_1 + a(X) f_2(X) u_2$$

4. if $\ell_1 > \ell_2$,

while $\left(f_1, (Y^{\ell_1 - \ell_2} + c, F)_Y\right) \neq 1$, do

$c :=$ random number $\in k$

5. $M_0 u := b(X) f_2(X) u_1 + a(X) f_1(X)(Y^{\ell_1 - \ell_2} + c) u_2$

6. if $\ell_2 > \ell_1$,

while $\left(f_2, (Y^{\ell_2 - \ell_1} + c, F)_Y\right) \neq 1$, do

$c :=$ random number $\in k$

7. $M_0 u := b(X) f_2(X)(Y^{\ell_2 - \ell_1} + c) u_1 + a(X) f_1(X) u_2$

8. $M_0(\mathfrak{a}_1 \cdot \mathfrak{a}_2) := (M_0 f, M_0 u)$.

Algorithm $M_1(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$

Let $\mathfrak{a}_1 = (f_1(X), u_1(X,Y))$, $\mathfrak{a}_2 = (f_2(X), u_2(X,Y))$ be invertible ideals where u_i's are monic polynomials in Y. Assume $\sqrt{(f_1)} = \sqrt{(f_2)}$.

1. $M_1 f := \dfrac{f_1 f_2}{(f_1, f_2)}$

$c := 0$

$d := 0$

$U_1 := u_1 + c f_1$

$U_2 := u_2 + d f_2$

$M_1 u := U_1 U_2$

2. $g_1 := (U_1, F)_Y \pmod{f_1^2}$

$g_2 := (U_2, F)_Y \pmod{f_2^2}$

3. while $f_1 \pmod{g_1} \neq 0$, do

$c :=$ random number $\in k$

4. while $f_2 \pmod{g_2} \neq 0$, do

$d :=$ random number $\in k$

5. $M_1(\mathfrak{a}_1 \cdot \mathfrak{a}_2) := (M_1 f, M_1 u)$

Algorithm $M(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$ (cf. 3.15)

Let $\mathfrak{a}_1 = (f_1(X), u_1(X,Y))$, $\mathfrak{a}_2 = (f_2(X), u_2(X,Y))$ be invertible ideals where u_i's are monic polynomials in Y.

1. $\ell_1 := \deg_Y f_1$

$\ell_2 := \deg_Y f_2$

$d(X) := (f_1, f_2)$

$f_{12} := (f_1, d^{\ell_1})$

$f_{22} := (f_2, d^{\ell_2})$

$f_{11} := \dfrac{f_1}{f_{12}}$

$f_{21} := \dfrac{f_2}{f_{22}}$

2. $(g_1, v_1) := M_0\left((f_{11}, u_1) \cdot (f_{21}, u_2)\right)$

$(g_2, v_2) := M_1\left((f_{12}, u_1) \cdot (f_{22}, u_2)\right)$

3. $M(\mathfrak{a}_1 \cdot \mathfrak{a}_2) := M_0\left((g_1, v_1) \cdot (g_2, v_2)\right)$

6. Conclusion and Forthcoming Problem

The heaviest part of the addition algorithm on $\mathrm{Pic}^0(C)$ is to compute the powers of a given element $\mathfrak{a} \in \mathrm{Pic}^0(C)$. As above, our proposal on the algorithm is to use the generaters of $\mathfrak{a}$ based on the plane coordinates (which we called a P-basis of $\mathfrak{a}$). Of course, those P-basis are not determined uniquely for a given $\mathfrak{a}$, but we insist that the algorithm using P-basis is faster than that using Gröbner basis.

To estimate our algorithm by some real examples is a very important task, which will appear in the near future.

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] S. Arita, S. Miura and T. Sekiguchi, *An addition algorithm on the Jacobian varieties of crves*, J. Ramanujan Math. Soc. 19(4), 1-17(2004)

[4] A. Basiri, A. Enge,J.-C. Faugère and N. Gürel, *The arithmetic of Jacobian groups of superelliptic cubics*, Mathematics of Computation, 74(249), 389-410(2004)

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

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

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

[8] R. Hartshorne, *Aalgebraic geometry*, Springer-Verlag, 1977

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

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

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

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

[13] 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)

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

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

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

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

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

(Shinji Miura) Research and Development Institute Chuo University, 1-13-27 Kasuga Bunkyo-ku Tokyo 112, Japan

E-mail address: smiura@tamacc.chuo-u.ac.jp

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

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