Yokohama Mathematical
Journal Vol. 69, 2023

DIFFERENTIAL FORMS ON THE CURVES ASSOCIATED TO APPELL-LAURICELLA HYPERGEOMETRIC SERIES AND THE CARTIER OPERATOR ON THEM

By

Ryo Ohashi and Shushi Harashita

(Received December 27, 2021; Revised November 25, 2023)

Abstract. The curve C over $\mathbb{C}$ associated to Appell-Lauricella hypergeometric series and regular differential forms on its desingularization were previously studied by Archinard. In this paper, we first generalize Archinard's results for a field K under a mild condition on its characteristic. Second, we describe a partial desingularization of C and the space of global sections of its dualizing sheaf, especially we give an explicit basis of it. Finally, when the characteristic is positive, we show that the Cartier operator on the space can be defined and describe it in terms of Appell-Lauricella hypergeometric series.

1. Introduction

Appell-Lauricella hypergeometric series is defined as a period of a family of degenerations of superelliptic curves, see Section 2 for the details. We are interested in relations between the geometry of the associated family of the (possibly singular) curves and the analysis of Appell-Lauricella hypergeometric series. Among them, we shall describe Cartier-Manin matrices of these curves in terms of Appell-Lauricella hypergeometric series (Theorem 6.5). To achieve this, we need to find explicit bases of the spaces of regular differential forms on the curves.

Let us start with recalling the most classical case: a relation between elliptic curves and Gauss' hypergeometric series. Gauss' hypergeometric series is defined to be

$$F(a, b, c\,; z) := \sum_{n=0}^{\infty} \frac{(a\,; n)(b\,; n)}{(c\,; n)(1\,; n)} z^n,$$

with $a, b, c \in \mathbb{C}$ and $-c \notin \mathbb{N}$, where $(x\,; n) = x(x+1)\cdots(x+n-1)$. It is

Key words and phrases: Algebraic curves, Cartier-Manin matrix, Cartier operator, Differential forms, Hypergeometric series, Positive characteristic

2020 Mathematics Subject Classification: 14H10, 14F40, 14G17, 33C70

well-known [23, Section 14.2] that $F(a,b,c\,;z)$ satisfies the differential equation $\mathcal{D}F(a,b,c\,;z)=0$ with

$$\mathcal{D}=z(1-z)\frac{d^2}{dz^2}+\big(c-(a+b+1)z\big)\frac{d}{dz}-ab. \tag{1.1}$$

It is also well-known [19, Theorem V.4.1] that the elliptic curve $E : y^2 = x(x-1)(x-z)$ in positive characteristic $p>0$ is supersingular if and only if $H_p(z)=0$, where

$$H_p(z) := \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 z^i.$$

In [12], Igusa proved that $H_p(z)$ is a separable polynomial, by using the fact that $H_p(z)$ satisfies the differential equation $\mathcal{D}'H_p(z)=0$ with

$$\mathcal{D}'=z(1-z)\frac{d^2}{dz^2}+(1-2z)\frac{d}{dz}-\frac{1}{4}. \tag{1.2}$$

Remark that (1.2) coincides with (1.1) for $(a,b,c)=(1/2,1/2,1)$, and $H_p(z)$ is obtained by truncating Gauss' hypergeometric series $F(1/2,1/2,1\,;z)$ at degree $(p-1)/2$. Also over $\mathbb{C}$, periods of the elliptic curve $y^2=x(x-1)(x-\lambda)$ are known [10, Chapter 9, Theoerm 6.1] to be described in terms of the hypergeometric series $F(1/2,1/2,1\,;\lambda)$. Some variants of hypergeometric series have sporadically been applied in situations involving higher genera; you can find examples in [11, Section 1.4], [3, Section 2], [22] and [17, Section 3].

In this paper, we study the curve C associated to Appell-Lauricella hypergeometric series (see Definition 2.3), which is a generalization of Gauss' hypergeometric series. The curve C is defined by the affine equation

$$C : y^N = f(x) := \prod_{i=0}^{r}(x-\lambda_i)^{A_i}, \quad i\neq j \Rightarrow \lambda_i\neq\lambda_j, \quad \lambda_0,\dots,\lambda_r\in\overline{K}, \tag{1.3}$$

with $(N,A_0,\dots,A_r)=1$. Here, the condition $(N,A_0,\dots,A_r)=1$ is necessary and sufficient for C to be irreducible (cf. Theorem 2.4).

The central purpose of this paper is to generalize the above result for elliptic curves to that for C and for (partial) desingularizations of C. When $A_0=\cdots=A_r=1$ and $N\geq 3$, the desingularization of C as in (1.3) is called *superelliptic*. As an extension of hyperelliptic curves, superelliptic curves have been important research objects (cf. González [5] and Sutherland [21] and so on). In general, for a study of a class of curves, one often need to explore degenerations of those curves. Consequently, it would be valuable to study curves in the form of (1.3), as they are degenerations of superelliptic curves.

On the other hand, the desingularization of C, say X, or partial desingularizations of C are worth studying not only as curves related to C but also as important examples of curves. Note that X is often called a cyclic cover of $\mathbb{P}^1$, as it is the nonsingular model whose function field is a cyclic cover of the function field of $\mathbb{P}^1$, see Bouw [2], Archinard [1] and Elkin [4] for related works.

Archinard [1, Section 2] described the desingularization X, especially over $\mathbb{C}$ and studied the space of regular differential forms on X. For our purpose, we first generalize Archinard's results to the case of a field K whose characteristic is not a divisor of N. The same statement without complete proof is found in Elkin [4, Section 2] and a similar result for the dual space (the first cohomology of X) is found in Bouw [2, Lemma 5.1]. In Section 2, we review fundamental properties of the curve C associated to Appell-Lauricella hypergeometric series, and construct the explicit desingularization map $\pi : X \to C$. In Section 3, we describe the space of regular differential forms on X. In the following, we choose a primitive N-th root ζ of unity.

Main Theorem A. *The regular differential module $\mathit{\Omega}[X]$ has a basis consisting of elements of the form*

$$\omega_{(s,\boldsymbol{a})} := \frac{\prod_{i=0}^{r}(x-\lambda_i)^{a_i}}{y^s}dx, \quad 0 \le s \le N-1,$$

where $\boldsymbol{a} = (a_0, \ldots, a_r)$ with $a_i \ge 0$. Moreover, assume that K contains $\lambda_0, \ldots, \lambda_r$ and ζ. For each $0 \le s \le N-1$, let V_s be the ζ^{-s}-eigenspace of the action on $\mathit{\Omega}[X]$ induced from the automorphism $(x, y) \mapsto (x, \zeta y)$ on X. Then $x^m \omega_{(s,\boldsymbol{e_s})}$ for $0 \le m \le d_s - 1$ form a basis of V_s, where

$$d_s = \max\left\{0, \left\lfloor \frac{s\sum A_k - (N, N-\sum A_k)}{N} \right\rfloor - \sum_{j=0}^{r} \left\lceil \frac{sA_j + (N, A_j)}{N} - 1 \right\rceil \right\},$$

$$e_{s,j} = \left\lceil \frac{sA_j + (N, A_j)}{N} - 1 \right\rceil \text{ with } \boldsymbol{e_s} = (e_{s,0}, e_{s,1}, \ldots, e_{s,r}).$$

As well as nonsingular curves, we often need to study singular curves. We shall deal with the curve C itself in Section 4 and the partial desingularization $\widetilde{C}$ only at ∞ in Section 5. In particular, the latter objects appear when we consider degenerations of hyperelliptic curves or superelliptic curves. The following two theorems provide explicit bases of the regular differential modules $\mathit{\Omega}[C]$ and $\mathit{\Omega}[\widetilde{C}]$ on C and $\widetilde{C}$ respectively, where the notion of regular differential forms of singular curves was defined by Serre [18, Section IV.3], see Section 4 for more details.

Main Theorem B. *Assume that K contains $\{\zeta, \lambda_0, \ldots, \lambda_r\}$. For $0 \le s \le N-1$, let W_s be the ζ^{-s}-eigenspace of the action on $\mathit{\Omega}[C]$ induced from the automorphism $(x, y) \mapsto (x, \zeta y)$ on C is given for each $0 \le s \le N-1$.*

(1) If $N - \sum A_k \geq 0$, then $x^i dx/y^s$ for $0 \leq i \leq s-2$ form a basis of W_s.
(2) If $N - \sum A_k < 0$, then $x^i y^{(j-1)N} dx/y^s$ for $0 \leq i \leq s - 2 - jN + \sum A_k$ and for $1 \leq j \leq \left\lfloor \dfrac{s-2+\sum A_k}{N} \right\rfloor$ form a basis of W_s.

Main Theorem C. *Assume that K contains $\{\zeta, \lambda_0, \dots, \lambda_r\}$. For $0 \leq s \leq N-1$, let $\widetilde{W_s}$ be the ζ^{-s}-eigenspace of the action on $\Omega[\widetilde{C}]$ induced from the automorphism $(x, y) \mapsto (x, \zeta y)$ on $\widetilde{C}$ is given for each $0 \leq s \leq N-1$. Then $x^{j-1}dx/y^s$ for $1 \leq j \leq \dfrac{s\sum A_k - (N, N - \sum A_k)}{N}$ form a basis of $\widetilde{W_s}$.*

As an application, in Section 6 we introduce the modified Cartier operator on the regular differential modules on X, C and $\widetilde{C}$ (Theorem 6.2). The last aim of this paper is to describe a relation between Appell-Lauricella hypergeometric series and the modified Cartier operator:

Main Theorem D. *Every component of Cartier-Manin matrices of X, C and $\widetilde{C}$ can be described by a truncation of Appell-Lauricella hypergeometric series. For the explicit formula, see Theorem 6.5.*

This result is a generalization of the fact that the x^{p-1}-coefficient of $\{x(x-1)(x-z)\}^{(p-1)/2}$ is equal to the truncation of $(-1)^{(p-1)/2}F(1/2, 1/2, 1\,; z)$ at degree $m = (p-1)/2$. The research of Cartier-Manin matrices (or their dual notion: Hasse-Witt matrices) has a long history. Among them, Sutherland provided a fast algorithm for computing Cartier-Manin matrices of superelliptic curves [21], also see [8] and [9] for hyperelliptic curves. This paper gives a formula of Cartier-Manin matrices whose entries are considered as polynomials in λ_i of (1.3). This result may not contribute to speeding up the computation if λ_i are constants, but it would have many applications if λ_i are indeterminates. In fact, Cartier-Manin matrices with polynomial entries are used in papers such as [13] and [14], for enumerating superspecial curves and proving the existence of supersingular curves.

This paper is organized as follows: In Section 2, we study the fundamentals of curves C associated to Appell-Lauricella hypergeometric series and provide the explicit desingularizations (we denote by X). Sections $3, 4$ and 5 are dedicated to describing the spaces of regular differential forms on X, C and $\widetilde{C}$, where $\widetilde{C}$ is the partial desingularization only at ∞. Finally in Section 6, we show that the modified Cartier operator stabilizes the spaces of regular differential forms on $\widetilde{C}$ and so on, and we elucidate the relation between the modified Cartier operator and Appell-Lauricella hypergeometric series.

Acknowledgements

The authors thank Yuya Yamamoto for pointing out some mistakes in an earlier version. They are also grateful to the referee for careful reading and helpful comments. This work was supported by JSPS Grant-in-Aid for Scientific Research (C) 17K05196, and 21K03159.

2. The curves associated to Appell-Lauricella hypergeometric series

In this section, we recall the definition of the curves associated to Appell-Lauricella hypergeometric series and some of their properties. Let K be a field.

Definition 2.1. Let N be a positive integer which is not a multiple of the characteristic of K. A *curve associated to Appell-Lauricella hypergeometric series* is the 1-dimensional algebraic set defined by

$$C : y^N = f(x)$$

for an $f(x) \in K[x]$, which is possibly inseparable: the polynomial $f(x)$ is factorized as

$$f(x) = \prod_{i=0}^{r} (x - \lambda_i)^{A_i}, \quad \lambda_0, \ldots, \lambda_r \in \overline{K},$$

where $A_i \geq 1$ and $\lambda_i \neq \lambda_j$ for $i \neq j$.

Remark 2.2. The curve C above (or more precisely, its desingularization) is called *superelliptic* if $A_i = 1$ for all $i \in \{0, \ldots, r\}$. If $N = 2$ and $r > 3$ in addition, the curve C is clearly hyperelliptic. Hence, a curve associated to Appell-Lauricella hypergeometric series is a certain generalization of these curves.

Definition 2.3. Appell-Lauricella hypergeometric series is defined to be

$$\mathcal{F}(a, b_1, \ldots, b_d, c\,; z_1, \ldots, z_d) := \sum_{n_1=0}^{\infty} \cdots \sum_{n_d=0}^{\infty} \frac{(a\,; \sum n_j) \prod (b_j\,; n_j)}{(c\,; \sum n_j) \prod (1\,; n_j)} \prod_{j=1}^{d} z_j^{n_j},$$

with $a, b_1, \ldots, b_d, c \in \mathbb{C}$ and $-c \notin \mathbb{N}$.

It is obvious that $\mathcal{F}(a, b, c\,; z) = F(a, b, c\,; z)$ when $d = 1$, and therefore the Appell-Lauricella hypergeometric series can be regarded as a certain generalization of Gauss' hypergeometric series. Moreover if $0 < \mathrm{Re}(a) < \mathrm{Re}(c)$, then it is known that $\mathcal{F}(a, b_2, \ldots, b_r, c\,; \lambda_2, \ldots, \lambda_r)$ has the integral representation as below:

$$\mathcal{F}(a, b_2, \ldots, b_r, c\,; \lambda_2, \ldots, \lambda_r) = \frac{\Gamma(c)}{\Gamma(a)\Gamma(c-a)} \int_1^\infty \prod_{i=0}^{r} (x - \lambda_i)^{-\mu_i} dx, \tag{2.1}$$

with $\lambda_0 = 0$ and $\lambda_1 = 1$, where $\mu_0 = c - \sum_{j=2}^{r} b_j$, $\mu_1 = 1 + a - c$ and $\mu_j = b_j$ for $j = 2, \ldots, r$. In the case where all μ_i are positive rational numbers, by setting the integrand of (2.1) as $1/y$, we see that the hypergeometric function is associated to the curve

$$y^N = \prod_{i=0}^{r} (x - \lambda_i)^{A_i},$$

where we set N to be the least common multiple of the denominators of $\mu_0, \ldots, \mu_r$ and we set $A_i = N\mu_i$ so that $(N, A_0, \ldots, A_r) = 1$ holds. We have a condition for C in Definition 2.1 to be irreducible:

Theorem 2.4 ([15, Chapter VI, Theorem 9.1])**.** *A curve C is irreducible over $\overline{K}$ (and hence over K) if and only if $(N, A_0, \ldots, A_r) = 1$.*

From now on, we assume that $(N, A_0, \ldots, A_r) = 1$, as we are specifically interested in studying the case where C is irreducible. Now we counsider C as a projective variety in $\mathbb{P}^2 = \operatorname{Proj} K[x_0, x_1, x_2]$. Set $A_\infty := \left| N - \sum_{k=0}^{r} A_k \right|$. The projective equation of C reads

- *Case 1:* $N - \sum_{k=0}^{r} A_k > 0$. $\quad {x_2}^N = {x_0}^{A_\infty} \prod (x_1 - \lambda_i x_0)^{A_i}$;
- *Case 2:* $N - \sum_{k=0}^{r} A_k < 0$. $\quad {x_2}^N {x_0}^{A_\infty} = \prod (x_1 - \lambda_i x_0)^{A_i}$;
- *Case 3:* $N - \sum_{k=0}^{r} A_k = 0$. $\quad {x_2}^N = \prod (x_1 - \lambda_i x_0)^{A_i}$.

Here, put $P_j = (1 : \lambda_j : 0)$ for $j \in \{0, \ldots, r\}$ and set $\mathcal{P}_{\text{fin}} := \{P_0, \ldots, P_r\}$. Put $P_\infty = (0 : 1 : 0)$ in *Case 1* and $P_\infty = (0 : 0 : 1)$ in *Case 2*. We set $\mathcal{P}_\infty := \{P_\infty\}$ for *Cases 1* and *2* and $\mathcal{P}_\infty := \emptyset$ for *Case 3*. Moreover, we set

$$\mathcal{P} := \mathcal{P}_{\text{fin}} \cup \mathcal{P}_\infty.$$

From the assumption that the characteristic of K is not a divisor of N, it is straightforward to see where C has singularities by using the Jacobian criterion:

Lemma 2.5. *Any singular point of C belongs to the set $\mathcal{P}$. Moreover C is singular at P_i for each $i \in \{0, \ldots, r, \infty\}$ if and only if $A_i > 1$.*

Next, we review the explicit description of the desingularization X of the curve C, as obtained by Archinard [1, Section 3.1], which works also in positive characteristic. Let $g_i = (N, A_i)$ for each $i \in \{0, \ldots, r, \infty\}$. Consequently,

$N_i = N/g_i$ and $A'_i = A_i/g_i$ are coprime non-negative integers. Thus, there exist $m_i, n_i \in \mathbb{Z}$ such that $m_i A'_i + n_i N_i = 1$.

Proposition 2.6 ([1, Section 3.1.1])**.** Suppose that the characteristic of K is equal to 0 or does not divide N. Let $j \in \{0, \ldots, r\}$ and define $f_j(x) := \prod_{i \neq j}(x - \lambda_i)^{A_i}$. Let $D(f_j)$ be the open subscheme obtained by excluding the part where $f_j(x) = 0$ from $\mathbb{A}^3 = \operatorname{Spec} K[x, u, z]$, and we set X_j to be the closed subscheme of $D(f_j)$ defined by

$$X_j : z^{N_j} = (x - \lambda_j)u^{m_j}, \ u^{g_j} = f_j(x).$$

Then, one can verify the nonsingularity of X_j using the Jacobian criterion. There exists a birational morphism

$$\pi_j : X_j \to C \smallsetminus \mathcal{P}_j \ ; \ (x, u, z) \mapsto (1 : x : u^{n_j} z^{A'_j}),$$

with $\mathcal{P}_j := \mathcal{P} \smallsetminus \{P_j\}$. Moreover π_j induces an isomorphism $X_j \smallsetminus \pi^{-1}(\{P_j\}) \xrightarrow{\cong} C \smallsetminus \mathcal{P}$, whose inverse is given by

$$\rho_j : C \smallsetminus \mathcal{P} \to X_j \smallsetminus \pi^{-1}(\{P_j\}) \, ; \, (1 : x : y) \mapsto (x, y^{N_j}(x - \lambda_j)^{-A'_j}, y^{m_j}(x - \lambda_j)^{n_j}).$$

Proposition 2.7 ([1, Section 3.1.2])**.** Suppose that the characteristic of K is equal to 0 or does not divide N. Put $f_\infty(\xi) := \prod_{i=0}^{r}(1 - \lambda_i \xi)^{A_i}$. We define X_∞, π_∞ in each case as follows. Then X_∞ is nonsingular, and birationally equivalent to C under a rational map π_∞.

- *Case 1:* $N - \sum A_k > 0$. In this case $x_\infty = x_0/x_1$ and $y_\infty = x_2/x_1$ are regular on P_∞. Let $D(f_\infty(x_\infty))$ be the open subscheme obtained by excluding the part where $f_\infty(x_\infty) = 0$ from $\mathbb{A}^3 = \operatorname{Spec} K[x_\infty, u, z]$, and we set X_∞ to be the closed subscheme of $D(f_\infty(x_\infty))$ defined by

  $$X_\infty : z^{N_\infty} = x_\infty u^{m_\infty}, \ u^{g_\infty} = f_\infty(x_\infty).$$

  Then, one can verify the nonsingularity of X_∞ by using the Jacobian criterion. There exists a birational morphism

  $$\pi_\infty : X_\infty \to C \smallsetminus \mathcal{P}_{\mathrm{fin}} \, ; \, (x_\infty, u, z) \mapsto (x_\infty : 1 : u^{n_\infty} z^{A'_\infty}),$$

  which induces an isomorphism $X_\infty \smallsetminus \pi^{-1}(\mathcal{P}_\infty) \xrightarrow{\cong} C \smallsetminus \mathcal{P}$, whose inverse is

  $$\rho_\infty : C \smallsetminus \mathcal{P} \to X_\infty \smallsetminus \pi^{-1}(\mathcal{P}_\infty) \, ; \, (x_\infty : 1 : y_\infty) \mapsto (x_\infty, \, x_\infty^{-A'_\infty} y_\infty^{N_\infty}, \, x_\infty^{n_\infty} y_\infty^{m_\infty}).$$

- *Case 2:* $N - \sum A_k < 0$. In this case $x_\infty = x_0/x_2$ and $y_\infty = x_1/x_2$ are regular on P_∞. Here, let $D(f_\infty(u))$ be the open subscheme obtained by excluding the part where $f_\infty(u) = 0$ from $\mathbb{A}^4 = \operatorname{Spec} K[u, v, w, z]$, and we set X_∞ to be the closed subscheme of $D(f_\infty(u))$ defined by

$$X_\infty : u = w^{m_\infty} z^{N_\infty},\ z^{A'_\infty} = v w^{n_\infty},\ w^{g_\infty} = f_\infty(u).$$

Then, one can verify the nonsingularity of X_∞ by using the Jacobian criterion. There exists a birational morphism

$$\pi_\infty : X_\infty \to C \smallsetminus \mathcal{P}_{\text{fin}}\,;\ (u, v, w, z) \mapsto (v w^{m_\infty} z^{N_\infty} : v : 1),$$

which induces an isomorphism $X_\infty \smallsetminus \pi^{-1}(\mathcal{P}_\infty) \xrightarrow{\cong} C \smallsetminus \mathcal{P}$, whose inverse is given by

$$\begin{aligned} C \smallsetminus \mathcal{P} &\to X_\infty \smallsetminus \pi^{-1}(\mathcal{P}_\infty)\,; \\ (x_\infty : y_\infty : 1) &\mapsto (x_\infty y_\infty^{-1},\ y_\infty,\ x_\infty^{A'_\infty} y_\infty^{-N_\infty - A'_\infty},\ x_\infty^{n_\infty} y_\infty^{m_\infty - n_\infty}). \end{aligned}$$

We note that in *Case 3*, the points at infinity $(0 : 1 : \zeta)$ with $\zeta^N = 1$ are all nonsingular as stated in Lemma 2.5. Hence, there is no need to consider X_∞ as Archinard excluded *Case 3*.

Remark 2.8. Note that X_i does not depend on the choice of m_i, n_i up to isomorphism. More precisely, suppose that (m'_i, n'_i) is another pair of integers satisfying $m'_i A'_i + n'_i N_i = 1$. Let X'_i be the set obtained from (m'_i, n'_i) in the same way, then X'_i is isomorphic to X_i. We give a proof of the case $i \in \{0, \dots, r\}$. Now, there is a relation $(n_i - n'_i)N_i = -(m_i - m'_i)A'_i$, then we have $e := (n_i - n'_i)/A'_i \in \mathbb{Z}$ since N_i and A'_i are coprime non-negative integers. Therefore, consider the morphism $X_i \to X'_i\,;\ (x, u, z) \mapsto (x, u, u^e z)$, which has the obvious inverse. Thus, we conclude that $X_i \cong X'_i$. The uniqueness of X_∞ can also be proved similarly.

Remark 2.9. The action on C by the group μ_N of N-th roots of unity, defined by $(x, y) \mapsto (x, \zeta y)$ for each $\zeta \in \mu_N$ can be extended to X_j as $(x, u, z) \mapsto (x,\ \zeta^{N_j} u,\ \zeta^{m_j} z)$. A similar extension applies to X_∞.

Now, we define the desingularization X of the curve C obtained by gluing $X_0, \dots, X_r, X_\infty$ along $X_i \smallsetminus \pi^{-1}(\{P_i\})$ and $X_j \smallsetminus \pi^{-1}(\{P_j\})$ via the isomorphisms

$$X_i \smallsetminus \pi^{-1}(\{P_i\}) \xrightarrow{\pi_i} C \smallsetminus \mathcal{P} \xleftarrow{\pi_j} X_j \smallsetminus \pi^{-1}(\{P_j\}).$$

By gluing maps $\pi_i : X_i \to C$, we also obtain a morphism $\pi : X \to C$ such that $\pi|_{X_i} = \pi_i$ for all $i \in \{0, \dots, r, \infty\}$. As can be found in [1, Section 3.2], this is indeed the desingularization of C under π. Moreover, the genus formula of X, as shown in the same manner as the case where $K = \mathbb{C}$, [1, Theorem 4.1], is as follows.

Theorem 2.10. The genus of X is given by

$$g(X) = 1 + \frac{1}{2}\Big(rN - \sum_{j=0}^{r}(N, A_j) - \big(N, N - \sum_{k=0}^{r} A_k\big)\Big).$$

Proof. Let $C \to \mathbb{P}^1$ be the projection $(x_0 : x_1 : x_2) \mapsto (x_0 : x_1)$ except for $(0 : 0 : 1) \mapsto (0 : 1)$ in *Case 2.* Composing this projection and $\pi : X \to C$, we obtain a finite separable morphism $X \to \mathbb{P}^1$.

point P of C	# of π-preimages Q of P	ramification index at Q
$(1 : \lambda_j : 0)$	(N, A_j)	$N/(N, A_j)$
∞	$(N, N - \sum A_k)$	$N/(N, N - \sum A_k)$
other points	1	1

The genus of the projective line $\mathbb{P}^1$ is 0, so we can directly see that $2g(X) - 2$ is equal to

$$-2N + \sum_{j=0}^{r}(N, A_j)\Big(\frac{N}{(N, A_j)} - 1\Big) + \big(N, N - \sum A_k\big)\Big(\frac{N}{(N, N - \sum A_k)} - 1\Big)$$
$$= rN - \big(N, N - \sum A_k\big) - \sum_{j=0}^{r}(N, A_j).$$

This is the desired conclusion. □

3. The space of regular differential forms on X

Let C be a curve over a field K as defined in Definition 2.1. In this section, for the desingularization map $\pi : X \to C$ constructed as in Section 2, we describe the regularity condition of rational differential forms on X. This enables us to provide an explicit basis of the space $\mathit{\Omega}[X]$ of regular differential forms on X, where "regular" is often called "of first kind". Note that $\mathit{\Omega}[X]$ is realized as a subspace of the space $\mathit{\Omega}(C)$ of rational differential forms on C.

A general idea to describe the space of differential forms on plane curves and the Cartier operator on it is found in Stöhr-Voloch [20]. As explained there, Gorenstein [6, Theorem 12] provides a description of regular differential forms on the projective smooth model of a plane curve $\mathit{\Gamma}$. However, our case does not satisfy his assumption: y is an integral element over $K(x)$. This would imply that the Zariski closure of $\mathit{\Gamma}$ in $\mathbb{P}^2$ is regular at every infinite place. In the following, we formulate a lemma that works in our case. First, let us review the result by Gorenstein:

Theorem 3.1 ([6, Theorem 12])**.** Let Γ be a plane curve $\operatorname{Spec} R$ with $R = K[x,y]/(F)$ where F is an irreducible element of degree m. Let L be the function field of Γ, and X be the nonsingular projective curve having the same function field L. Assume that x, considered as an element of L is transcendental over K and y, considered as an element of L, is separable over $K(x)$. A rational differential form ω is regular on X if and only if it can be written in the form

$$\frac{\phi(x,y)}{(\partial F/\partial y)(x,y)}dx$$

such that $\phi(x,y)$ is an *adjoint element* of degree h, whose precise meaning is

(i) $\phi(x,y) \in \mathfrak{C}$, where $\mathfrak{C}$ is the conductor of $R = K[x,y]/(F)$ in the integral closure $\overline{R}$ of R in L (i.e. $\mathfrak{C} := \{z \in R\,;\, z\overline{R} \subset R\}$).

(ii) $\phi'(x',y')(x')^{\mathrm{m}-3-\mathrm{h}} \in \mathfrak{C}'$, where ϕ' be the polynomial in x' and y' defined by $\phi(x,y) = \phi'(x',y')/(x')^{\mathrm{h}}$ with $(x',y') = (1/x, y/x)$ and $\mathfrak{C}'$ is the conductor of $R' = K[x',y']/(F')$ with $F(x,y) = F'(x',y')/(x')^{\mathrm{m}}$ in the integral closure $\overline{R'}$ of R' in L.

(iii) $\phi''(x'',y'')(y'')^{\mathrm{m}-3-\mathrm{h}} \in \mathfrak{C}''$, where ϕ'' be the polynomial in x'' and y'' defined by $\phi(x,y) = \phi''(x'',y'')/(y'')^{\mathrm{h}}$ with $(x'',y'') = (x/y, 1/y)$ and $\mathfrak{C}''$ is the conductor of $R'' = K[x'',y'']/(F'')$ with $F(x,y) = F''(x'',y'')/(y'')^{\mathrm{m}}$ in the integral closure $\overline{R''}$ of R'' in L.

Remark 3.2. Here $\phi(x,y) \in \mathfrak{C}$ is equivalent to $\phi(x,y) \in \mathfrak{C}_P := \{z \in R_P\,;\, z\overline{R_P} \subset R_P\}$ for maximal ideal P of R, where $\overline{R_P}$ is the integral closure of R_P in L. Moreover $\mathfrak{C}_P = {\mathfrak{C}_P}^* \cap R_P$, where $\mathfrak{C}_P^*$ is the conductor of $(R_P)^*$ in $(\overline{R_P})^*$ (cf. [6, Theorem 2]). Here $*$ means taking the completion. If the Zariski closure of Γ in $\mathbb{P}^2$ is regular at every infinite place, (i) and (ii) in Theorem 3.1 can be replaced by $\mathrm{h} \le \mathrm{m} - 3$.

Now, let us return to our case $F = y^N - f(x)$. Our aim is to find a basis of the regular differential module $\Omega[X]$. Our method consists of three steps: The first step (Lemma 3.3) demonstrates that $\Omega[X]$ can be generated by differential forms of a specific form. However, these forms may not be regular at some specific points of X. Therefore, in the second step (Propositions 3.4 and 3.5) we give a criterion for determining whether a differential form of this kind is regular at those points. In the final step (Theorem 3.6), by combining these results we will derive an explicit basis of $\Omega[X]$. In the following, let μ_N be the subgroup of $\overline{K}^\times$ consisting of N-th roots of unity. We assume that K contains μ_N and the set $\{\lambda_0, \dots, \lambda_r\}$.

Lemma 3.3. The regular differential module $\Omega[X]$ is generated over K by elements of the form

$$\omega_{(s,\boldsymbol{a})} := \frac{\prod_{i=0}^{r}(x-\lambda_i)^{a_i}}{y^s}dx,$$

where $0 \leq s \leq N-1$ and $\boldsymbol{a} = (a_0, \ldots, a_r)$ with $a_i \geq 0$.

Proof. We use the notation from Theorem 3.1: $R = K[x,y]/(F)$ with $F = y^N - f(x)$. Let $\phi(x,y)$ be an adjoint element as defined in Theorem 3.1. By using $y^N = f(x)$, one can write

$$\phi(x,y) = \phi_0(x) + \phi_1(x)y + \cdots + \phi_{N-1}(x)y^{N-1},$$

with $\phi_j(x) \in K[x]$. Consider the action of the group μ_N on R given by $(x,y) \mapsto (x, \zeta y)$ for $\zeta \in \mu_N$. Since this action stabilizes $\mathfrak{C}$, $\mathfrak{C}'$ and $\mathfrak{C}''$, we obtain that $\phi(x, \zeta y)$ is also an adjoint element for all $\zeta \in \mu_N$. This implies that each term $\phi_j(x)y^j$ is an adjoint element. Clearly $\phi_j(x)$ can be uniquely written as $\varphi(x)\prod_{i=0}^{r}(x-\lambda_i)^{a_i}$, where $\varphi(x)$ is coprime to $x - \lambda_i$ for $i = 0, 1, \ldots, r$. As we can check that $\phi_j(x)y^j \in \mathfrak{C}$ by looking at whether $\phi_j(x)y^j \in \mathfrak{C}_P$ for all $P \in \{P_0, \ldots, P_r\}$, we conclude that $\varphi(x)\prod_{i=0}^{r}(x-\lambda_i)^{a_i}y^j \in \mathfrak{C}$ if and only if $\prod_{i=0}^{r}(x-\lambda_i)^{a_i}y^j \in \mathfrak{C}$. At an infinite place, the condition (ii) and (iii) of Theorem 3.1 can be described as the degree of ϕ_j being less than or equal to a certain constant depending only on C (see Proposition 3.5 below). Hence, if $\varphi(x)\prod_{i=0}^{r}(x-\lambda_i)^{a_i}y^j$ is an adjoint element, then $\prod_{i=0}^{r}(x-\lambda_i)^{a_i}y^j \in \mathfrak{C}$ is also an adjoint element. Thus, we have the lemma. □

Note that $\pi^*\omega_{(s,\boldsymbol{a})}$ is regular at every finite place except $Q_i \in \pi^{-1}(\{P_i\})$ for $i = 0, \ldots, r$. Let us find the condition for $\pi^*\omega_{(s,\boldsymbol{a})}$ to be regular at $Q_i \in \pi^{-1}(\{P_i\})$.

Proposition 3.4. For each $j \in \{0, \ldots, r\}$, the pull-back $\pi^*\omega_{(s,\boldsymbol{a})} \in \Omega(X)$ is regular at the place $Q_j \in \pi^{-1}(\{P_j\})$ if and only if

$$a_j \geq \frac{sA_j + (N, A_j)}{N} - 1.$$

Proof. The equations defining X_j gives other equations

$$\begin{aligned} N_j z^{N_j-1}dz &= u^{m_j}dx + m_j(x-\lambda_j)u^{m_j-1}du, \\ g_j u^{g_j-1}du &= (df_j/dx)dx. \end{aligned}$$

By $\pi^*(x) = x$ and $\pi^*(y) = u^{n_j}z^{A'_j}$ with $\pi^*(x - \lambda_j) = u^{-m_j}z^{N_j}$, a direct calculation shows that

$$\pi^*\omega_{(s,\boldsymbol{a})} = \frac{Nu^{g_j - sn_j - (1+a_j)m_j}z^{-sA'_j + (1+a_j)N_j - 1}\prod_{i\neq j}(x-\lambda_i)^{a_i}}{g_j f_j(x) + m_j(x-\lambda_j)(df_j/dx)}dz. \tag{3.1}$$

Hence $\pi^*\omega_{(s,\boldsymbol{a})}$ is regular at Q_j if and only if $-sA'_j + (1+a_j)N_j - 1 \geq 0$. □

Similarly, the regularity at the infinite place is described as below:

Proposition 3.5. The pull-back $\pi^*\omega_{(s,\boldsymbol{a})} \in \Omega(X)$ is regular at the place $Q_\infty \in \pi^{-1}(\{P_\infty\})$ in *Cases 1* and *2* and at the place $Q_\infty \in \pi^{-1}(\{(0:1:\zeta)\,;\,\zeta^N = 1\})$ in *Case 3* if and only if

$$\sum_{k=0}^{r} a_k \leq \frac{s\sum A_k - (N, N - \sum A_k)}{N} - 1.$$

Proof. In each case, we can write $\omega_{(s,\boldsymbol{a})} = {x_0}^{s-\sum a_k - 2}{x_2}^{-s}\prod(x_1 - \lambda_i x_0)^{a_i}(x_0dx_1 - x_1dx_0)$.

- *Case 1:* $N - \sum A_k > 0$. In this case, recall that $x_\infty = x_0/x_1$ and $y_\infty = x_2/x_1$; one can check that
$$\omega_{(s,\boldsymbol{a})} = -x_\infty^{s-\sum a_k-2}y_\infty^{-s}\prod(1-\lambda_i x_\infty)^{a_i}dx_\infty.$$
The equations defining X_∞ give other equations
$$N_\infty z^{N_\infty-1}dz = u^{m_\infty}dx_\infty + m_\infty x_\infty u^{m_\infty-1}du,$$
$$g_\infty u^{g_\infty-1}du = (df_\infty/dx_\infty)dx_\infty.$$
By using $\pi^*(x_\infty) = x_\infty$ and $\pi^*(y_\infty) = u^{n_\infty}z^{A'_\infty}$, we see that $\pi^*\omega_{(s,\boldsymbol{a})}$ is equal to
$$\frac{-Nu^{g_\infty - s(m_\infty+n_\infty)+(1+\sum a_k)m_\infty}z^{s(N_\infty - A'_\infty)-(1+\sum a_k)N_\infty - 1}\prod(1-\lambda_i x_\infty)^{a_i}}{g_\infty f_\infty(x_\infty) + m_\infty x_\infty(df_\infty(x_\infty)/dx_\infty)}dz. \tag{3.2}$$
Hence $\pi^*\omega_{(s,\boldsymbol{a})}$ is regular at Q_∞ if and only if $s(N_\infty - A'_\infty) - (1+\sum a_k)N_\infty - 1 \geq 0$.
- *Case 2:* $N - \sum A_k < 0$. In this case, recall that $x_\infty = x_0/x_2$ and $y_\infty = x_1/x_2$; one can check that
$$\omega_{(s,\boldsymbol{a})} = x_\infty^{s-\sum a_k - 2}\prod(y_\infty - \lambda_i x_\infty)^{a_i}(x_\infty dy_\infty - y_\infty dx_\infty).$$
The equations defining X_∞ give other equations
$$A'_\infty u^{A'_\infty - 1}du = N_\infty v^{N_\infty - 1}wdv + v^{N_\infty}dw,$$
$$A'_\infty z^{A'_\infty - 1}dz = w^{n_\infty}dv + n_\infty v w^{n_\infty - 1}dw,$$
$$g_\infty w^{g_\infty - 1}dw = (df_\infty(u)/du)du.$$
A tedious computation with these equations show that $\pi^*\omega_{(s,\boldsymbol{a})}$ is equal to
$$\frac{Nw^{g_\infty + s(m_\infty - n_\infty)-(1+\sum a_k)m_\infty}z^{s(N_\infty + A'_\infty)-(1+\sum a_k)N_\infty - 1}\prod(1-\lambda_i u)^{a_i}}{m_\infty u(df_\infty(u)/du) - g_\infty f_\infty(u)}dz. \tag{3.3}$$

Hence $\pi^*\omega_{(s,\boldsymbol{a})}$ is regular at Q_∞ if and only if

$$s(N_\infty + A'_\infty) - (1 + \sum a_k)N_\infty - 1 \geq 0.$$

- *Case 3:* $N - \sum A_i = 0$. In this case, we put $y_\infty = x_2/x_1$ and $z = x_0/x_1$. Then, one can check that $\pi^*(\omega_{s,\boldsymbol{a}})$ is given as

  $$\pi^*\omega_{(s,\boldsymbol{a})} = \frac{-z^{s-\sum a_i - 2}\prod(1-\lambda_i z)^{a_i}}{y_\infty^s}dz.$$

  Hence $\pi^*(\omega_{s,\boldsymbol{a}})$ is regular at $Q_\infty \in \pi^{-1}(\{(0:1:\zeta)\,;\,\zeta^N = 1\})$ if and only if $s - \sum a_i - 2 \geq 0$.

Thus the proposition holds in every case. □

With the discussions above, we can characterize the regular differential module $\mathit{\Omega}[X]$.

Theorem 3.6. Assume that K contains μ_N and $\{\lambda_0, \dots, \lambda_r\}$. For $0 \leq s \leq N-1$, let V_s be the subspace of $\mathit{\Omega}[X]$ with the character $\zeta \mapsto \zeta^s$ under the action $(x, y) \to (x, \zeta y)$ of μ_n on the regular differential module $\mathit{\Omega}[X]$. Note that $\mathit{\Omega}[X] = V_0 \oplus \cdots \oplus V_{N-1}$. Put

$$d_s = \max\left\{0, \left\lfloor \frac{s\sum A_k - (N, N - \sum A_k)}{N} \right\rfloor - \sum_{j=0}^{r} \left\lceil \frac{sA_j + (N, A_j)}{N} - 1 \right\rceil \right\},$$

$$e_{s,j} = \left\lceil \frac{sA_j + (N, A_j)}{N} - 1 \right\rceil \text{ with } \boldsymbol{e_s} = (e_{s,0}, e_{s,1}, \dots, e_{s,r}).$$

Then, we have $\dim V_s = d_s$. Moreover, a basis of V_s is given by

$$x^m\omega_{(s,\boldsymbol{e_s})} = x^m \frac{\prod_{j=0}^r (x-\lambda_j)^{e_{s,j}}}{y^s} dx$$

for $0 \leq m \leq d_s - 1$.

Proof. It is obvious that $x^m\omega_{(s,\boldsymbol{e_s})} \in V_s$ for all $0 \leq m \leq d_s - 1$, since x^m is a linear combination of $(x-\lambda_0)^k$ for $0 \leq k \leq m$ and for $\boldsymbol{a} = \boldsymbol{e_s} + (k, 0, \dots, 0)$, so we have $\omega_{(s,\boldsymbol{a})} \in \mathit{\Omega}[X]$ by Proposition 3.4 and Proposition 3.5. For the converse, any element of V_s is a linear combination of $\omega_{(s,\boldsymbol{a})}$ with $a_j \geq e_{s,j}$ for all $j \in \{0, \dots, r\}$ and

$$\sum_{k=0}^{r} a_k \leq \left\lfloor \frac{s\sum A_k - (N, N - \sum A_k)}{N} \right\rfloor - 1.$$

By rewriting $\omega_{(s,\boldsymbol{a})} = \varphi(x)\omega_{(s,\boldsymbol{e_s})}$ with $\deg\varphi \leq d_s - 1$, the space of such $\varphi(x)$ is spanned by $\{1, x, \dots, x^{d_s - 1}\}$. It is clear that $x^m\omega_{(s,\boldsymbol{e_s})}$ for $m = 0, \dots, d_s - 1$ are linearly independent. □

Summarizing the discussions above, we obtain Main Theorem A in Section 1.

Remark 3.7. If K is a perfect field and contains μ_N consisting of N-th roots of unity, then each member of the basis obtained above is defined over K. In fact, since $\omega_{(s,\boldsymbol{e_s})}$ is the unique “monic” element with the lowest-degree, it is stable under the action of $\mathrm{Gal}(\overline{K}/K)$.

4. The space of regular differential forms on C

In this section, we consider regular differential forms on C. As we have seen in Lemma 2.5, the curve C has singularities. We refer to [18, Chapter IV, §3.9] for the regular differential forms of singular curves. Let us give a brief review of it. We set $\varOmega[C] := \bigcap_{P\in C} \varOmega[C]_P$ with

$$\varOmega[C]_P := \left\{ \omega \in \varOmega(X); \sum_{\pi(Q)=P} \mathrm{res}_Q(\pi^*(h)\omega) = 0, \text{for all } h \in \mathcal{O}_{C,P} \right\}, \tag{4.1}$$

where $\pi : X \to C$ is the desingularization map constructed in Section 2. We note that $\varOmega[C]_P$ is an $\mathcal{O}_{C,P}$-module, and furthermore $\varOmega[C]$ is the space of global sections of the sheaf $U \mapsto \bigcap_{P\in U} \varOmega[C]_P$, which turns out to be the dualizing sheaf on C. First, we examine $\varOmega[C]_{P_j}$ for $j = 0, \ldots, r$. We use the notations introduced in Proposition 2.6.

Lemma 4.1. For $j \in \{0, \ldots, r\}$, we set $d \geq 0$ and $e \in \{1, \ldots, g_j\}$. A differential form $u^{g_j - e} dz/z^{d+1}$ belongs to $\varOmega[C]_{P_j}$ if and only if any pair (a, b) of non-negative integers does not satisfy

$$\begin{cases} aN_j + bA'_j = d, \\ -am_j + bn_j \equiv e \pmod{g_j}. \end{cases}$$

Proof. Any element of $\mathcal{O}_{C,P_j}$ can be written as αh where $\alpha \in \mathcal{O}_{C,P_j}^\times$ and $h = (x - \lambda_j)^a y^b$ for non-negative integers a and b. Recall that $\pi^*(x - \lambda_j) = u^{-m_j} z^{N_j}$ and $\pi^*(y) = u^{n_j} z^{A'_j}$. Thus, we have

$$\pi^*(h) u^{g_j - e} dz/z^{d+1} = u^{-am_j + bn_j + g_j - e} z^{aN_j + bA'_j} dz/z^{d+1}.$$

The sum of the residues at the point $Q_j = (\lambda_j, u, 0) \in \pi^{-1}(\{P_j\})$, where u runs among the g_j-th roots of $f_j(\lambda_j)$, is non-zero if and only if $aN_j + bA'_j = d$ and $-am_j + bn_j \equiv e \pmod{g_j}$. □

According to Lemma 4.1 and Proposition A.4, we directly obtain the following:

(i) if $d \geq g_j N_j A'_j - N_j - A'_j + 1$, then $u^{g_j - e} dz/z^{d+1} \notin \Omega[C]_{P_j}$ for all $e \in \{1, \dots, g_j\}$.

(ii) for $d_0 = g_j N_j A'_j - N_j - A'_j$ and $e_0 \equiv m_j - n_j \pmod{g_j}$, we see that $u^{g_j - e_0} dz/z^{d_0+1}$ belongs to $\Omega[C]_{P_j}$. Since $u^{g_j} = f_j(x) \in \mathcal{O}_{C,P_j}^{\times}$, there is no need to be concerned about the choice of e_0.

Moreover, we have the following:

(iii) the differential form $u^{g_j - e_0} dz/z^{d_0+1}$ in (ii) is a generator of $\Omega[C]_{P_j}$. Indeed, according to Lemma 4.1 and Proposition A.5, any differential form $u^{g_j - e} dz/z^{d+1} \in \Omega[C]_{P_j}$ can be written as $(x - \lambda_j)^{a'} y^{b'} u^{g_j - e_0} dz/z^{d_0+1}$ for non-negative integers a' and b', up to a multiple of an element of $\mathcal{O}_{C,P_j}^{\times}$.

Let us rewrite a generator of $\Omega[C]_{P_j}$.

Lemma 4.2. For $j \in \{0, \dots, r\}$, the pull-back $\pi^*(dx/y^{N-1})$ is a generator of $\Omega[C]_{P_j}$.

Proof. By (3.1), the pull-back $\pi^*(dx/y^{N-1}) = \pi^* \omega_{(N-1,\mathbf{0})}$ is equal to

$$u^{g_j - (N-1)n_j - m_j} z^{-(N-1)A'_j + N_j - 1} dz$$

up to a multiple of an element of $\mathcal{O}_{C,P_j}^{\times}$. This is the same form as in (ii) above. □

Next, we describe a generator of $\Omega[C]_{P_\infty}$. Here, we use the notation from Proposition 2.7. In *Case 1*, Lemma 4.1 holds after replacing j by ∞. Therefore, we similarly obtain the following:

(i) if $d \geq g_\infty N_\infty A'_\infty - N_\infty - A'_\infty + 1$, then $u^{g_\infty - e} dz/z^{d+1} \notin \Omega[C]_{P_\infty}$ for all $e \in \{1, \dots, g_\infty\}$.

(ii) for $d_0 = g_\infty N_\infty A'_\infty - N_\infty - A'_\infty$ and $e_0 \equiv m_\infty - n_\infty \pmod{g_\infty}$, we have that $u^{g_\infty - e_0} dz/z^{d_0+1}$ belongs to $\Omega[C]_{P_\infty}$.

(iii) the differential form $u^{g_\infty - e_0} dz/z^{d_0+1}$ in (ii) is a generator of $\Omega[C]_{P_\infty}$.

Lemma 4.3. In *Case 1*, the pull-back $\pi^* \omega_{(N-1,\boldsymbol{a})}$ is a generator of $\Omega[C]_{P_\infty}$ if $\sum a_k = N - 3$.

Proof. By (3.2), the pull-back $\pi^* \omega_{(N-1,\boldsymbol{a})}$ with $\sum a_k = N - 3$ is equal to

$$u^{g_\infty - (N-1)n_\infty - m_\infty} z^{(N-1)A'_\infty + N_\infty - 1} dz$$

up to a multiple of an element of $\mathcal{O}_{C,P_\infty}^{\times}$. This is the same form as in (ii) above. □

In *Case 2*, we set $N'_\infty := N_\infty + A'_\infty$. Then, Lemma 4.1 holds after replacing N_j by N'_∞ and j by ∞. We similarly obtain the following:

(i) if $d \geq g_\infty N'_\infty A'_\infty - N'_\infty - A'_\infty + 1$, then $w^{g_\infty - e} dz/z^{d+1} \notin \Omega[C]_{P_\infty}$ for all $e \in \{1, \dots, g_\infty\}$;

(ii) for $d_0 = g_\infty N'_\infty A'_\infty - N'_\infty - A'_\infty$ and $e_0 \equiv 2n_\infty - m_\infty \pmod{g_\infty}$, we have that $w^{g_\infty - e_0} dz/z^{d_0+1}$ belongs to $\Omega[C]_{P_\infty}$;

(iii) the differential form $w^{g_\infty - e_0} dz/z^{d_0+1}$ in (ii) is a generator of $\Omega[C]_{P_\infty}$.

Lemma 4.4. In *Case 2*, the pull-back $\pi^* \omega_{(2-A_\infty, \boldsymbol{a})}$ is a generator of $\Omega[C]_{P_\infty}$ if $\sum a_k = 0$.

Proof. By (3.3), the pull-back $\pi^* \omega_{(2-A_\infty, \boldsymbol{a})}$ with $\sum a_k = 0$ is equal to

$$w^{g_\infty - (2-A_\infty)n_\infty + (1-A_\infty)m_\infty} z^{(2-A_\infty)(N_\infty + A'_\infty) - N_\infty - 1} dz$$

up to a multiple of an element of $\mathcal{O}^\times_{C, P_\infty}$. This is the same form as in (ii) above. □

We obtain the regularity of certain rational differential forms on C, which will turn out to form a basis of the space of regular differential forms on C (cf. Corollary 4.6).

Theorem 4.5. We have the following statements:

(1) Assume $N - \sum A_k \geq 0$. Then, for $0 \leq s \leq N-1$, we have $\omega_{(s, \boldsymbol{a})} \in \Omega[C]$ if
  (i) $a_j \geq 0$ for all $j \in \{0, \dots, r\}$ and
  (ii) $0 \leq \sum a_k \leq s - 2$.

(2) Assume $N - \sum A_k < 0$. Then, for $2 - A_\infty \leq s \leq N-1$, we have $\omega_{(s, \boldsymbol{a})} \in \Omega[C]$ if
  (i) $a_j \geq 0$ for all $j \in \{0, \dots, r\}$ and
  (ii) $0 \leq \sum a_k \leq s - 2 + A_\infty$.

Proof. First of all, recall that the differential form dx/y^{N-1} and its products of some x and y are regular at P_j for $j \in \{0, \dots, r\}$, by Lemma 4.2.

(1) The differential form $\omega_{(N-1, \boldsymbol{a}')}$ for $\sum a'_k = N-3$ and its products of some $1/x$ and y/x are regular at P_∞, by Lemma 4.3 in *Case 1*. Then, the theorem in this case follows from the fact that $\omega_{(s, \boldsymbol{a})}$ for $\boldsymbol{a}$ satisfying (i) and (ii) is a linear combination of

$$\left(\frac{1}{x}\right)^i \left(\frac{y}{x}\right)^{N-1-s} \frac{x^{N-3} dx}{y^{N-1}}$$

for $0 \leq i \leq s-2$. In *Case 3*, recall that P_∞ are all nonsingular points, as noted in Lemma 2.5. Consequently, $\Omega[C]_{P_\infty}$ is the set of regular differential forms at the point $Q_\infty \in \pi^{-1}(\{P_\infty\})$. Therefore, this case follows from (3.4).

(2) The differential form $\omega_{(2-A_\infty,\boldsymbol{a}')}$ where $\sum a'_k = 0$ and its products of some $1/y$ and x/y are regular at P_∞, by Lemma 4.4 in *Case 2.* Then, the theorem in this case follows from the fact that $\omega_{(s,\boldsymbol{a})}$ for $\boldsymbol{a}$ satisfying (i) and (ii) is a linear combination of

$$\left(\frac{1}{y}\right)^i \left(\frac{x}{y}\right)^{s-2+A_\infty-i} \frac{dx}{y^{2-A_\infty}}$$

for $0 \le i \le s-2+A_\infty$. □

Let μ_N be the subgroup of $\overline{K}^\times$ consisting of N-th roots of unity. For each $\zeta \in \mu_N$, we have the automorphism of C defined by $(x,y) \mapsto (x,\zeta y)$, which is extended to an automorphism of X, denoted as ι_ζ. This induces an action of μ_N on $\Omega[C]$. Specifically, ι_ζ stabilizes the place P_j and induces a permutation of $\pi^{-1}(\{P_j\})$. Moreover, we have $\mathrm{res}_Q(\omega) = \mathrm{res}_{\iota_\zeta(Q)}(\iota_\zeta{}^*\omega)$ for each $Q \in \pi^{-1}(\{P_j\})$, thanks to Remark 2.9.

Corollary 4.6. Assume that K contains μ_N and $\{\lambda_0,\dots,\lambda_r\}$. For $0 \le s \le N-1$, let W_s be the subspace of $\Omega[C]$ consisting of $\omega \in \Omega[C]$ on which μ_N acts by $\omega \mapsto \zeta^s\omega$ for all $\zeta \in \mu_N$.

(1) If $N - \sum A_k \ge 0$, then

$$\{x^i dx/y^s\,;\, 0 \le i \le s-2\} \tag{4.2}$$

is a basis of W_s. In particular

$$\dim W_s = s-1$$

with $\dim \Omega[C] = (N-1)(N-2)/2$.

(2) If $N - \sum A_k < 0$, then

$$\left\{x^i y^{(j-1)N} dx/y^s\,;\, 0 \le i \le s-2-jN+\sum A_k,\ 1 \le j \le \left\lfloor \frac{s-2+\sum A_k}{N} \right\rfloor \right\} \tag{4.3}$$

is a basis of W_s. In particular

$$\dim W_s = \sum_{j=1}^{\left\lfloor \frac{s-2+\sum A_k}{N} \right\rfloor} \left(s-1-jN+\sum A_k\right) \tag{4.4}$$

with $\dim \Omega[C] = (-1+\sum A_k)(-2+\sum A_k)/2$.

Proof. (1) The differential forms in (4.2) belong to W_s by using Theorem 4.5 (1), and they are linear independent. Using [7, Corollary III.9.10], we know that the arithmetic genus does not change among fibers of a flat family over a connected Noetherian scheme; therefore, neither does the dimension of the space of global sections of the dualizing sheaf [7, Chapter III, §7]. Here, consider the family

$$y^N = \prod_{j=0}^{r}\prod_{k=1}^{A_j}(x-\gamma_{jk}z)\cdot\prod_{l=1}^{A_\infty}(-a_l x+z),$$

which has C as a special fiber (defined by $\gamma_{jk}=\lambda_j$ and $a_l=0$). Since its generic fiber has the arithmetic genus $(N-1)(N-2)/2=\sum(s-1)$, the differential forms in (4.2) span W_s.

(2) The differential forms in (4.3) belong to W_s by using Theorem 4.5 (2), and they are linear independent. Similar to (1), consider the projective model of C:

$$y^N z^{A_\infty} = \prod_{j=1}^{r}(x-\lambda_j z)^{A_j}$$

deforms to a smooth curve of degree $\sum A_k$, we have

$$\dim \varOmega[C] = \left(-1+\sum A_k\right)\left(-2+\sum A_k\right)/2.$$

Hence, it suffices to show that the sum of the right hand side of (4.4) for $s=0,\dots,N-1$ is equal to $(-1+\sum A_k)(-2+\sum A_k)/2$ to prove (4.4). This follows from the fact that the set

$$\left\{s-1-jN+\sum A_k\ ;\ 0\le s\le N-1, 1\le j\le \left\lfloor\frac{s-2+\sum A_k}{N}\right\rfloor\right\}$$

is equal to $\{1,\dots,-2+\sum A_k\}$, since $1\le s-1-jN+\sum A_k\le -2+\sum A_k$. □

Summarizing the discussions above, we obtain the Main Theorem B in Section 1. In the last part of this section, we provide an example of regular differential forms on a singular curve:

Example 4.7. Let $C: y^3 = x(x-1)^2(x-z)^2$ and let X be the desingularizaiton of C. Then,

$$\left\{dx,\ \frac{dx}{y},\ \frac{xdx}{y},\ \frac{dx}{y^2},\ \frac{xdx}{y^2},\ \frac{x^2dx}{y^2}\right\}$$

forms a basis of $\varOmega[C]$, while $dx/y, x^2dx/y^2\in\varOmega[X]$.

5. The space of regular differential forms on $\widetilde{C}$

One can consider partial desingularizations of C, i.e., the desingularization only around a subset of $\mathcal{P} = \{P_0, \ldots, P_r, P_\infty\}$. Avoiding the general setting, in this section we focus on the desingularization $\widetilde{C}$ only around P_∞ of the curve C in *Cases 1* and *2*, which is the most interesting case. We exclude *Case 3*, since $\widetilde{C} = C$ by using Lemma 2.5 in this case. Our aim in this section is to give an explicit basis of the space of the regular differential forms on $\widetilde{C}$. Now, $\widetilde{C}$ is described as follows:

Definition 5.1. Let C be a curve associated to Appell-Lauricella hypergeometric series as in Definition 2.1. Then, we define $\widetilde{C}$ by gluing X_∞ and $C \smallsetminus \{P_\infty\}$.

Next, let us construct the morphism $\widetilde{\pi} : X \to \widetilde{C}$ as follows: We recall that the complete desingularization X was defined by gluing X_i in Section 2. Therefore, it suffices to define the morphism $\widetilde{\pi}_i : X_i \to \widetilde{C}$ for each $i \in \{0, \ldots, r, \infty\}$.

- For $j \in \{0, \ldots, r\}$, we define $\widetilde{\pi}_j$ to be the composition of $\pi_j : X_i \to C \smallsetminus \{P_0, \overset{j}{\overset{\vee}{\ldots}}, P_r, P_\infty\}$ and the inclusion $C \smallsetminus \{P_0, \overset{j}{\overset{\vee}{\ldots}}, P_r, P_\infty\} \to C \smallsetminus \{P_\infty\}$.
- We define $\widetilde{\pi}_\infty$ to be the inclusion $X_\infty \to \widetilde{C}$.

Here is a description of the regularity of differential forms on $\widetilde{C}$ and an explicit basis of $\Omega[\widetilde{C}]$.

Theorem 5.2. We have $\widetilde{\pi}^* \omega_{(s,\boldsymbol{a})} \in \Omega[\widetilde{C}]$ if

(i) $a_j \geq 0$ for all $j \in \{0, \ldots, r\}$ and

(ii) $0 \leq \sum a_k \leq \dfrac{s \sum A_k - (N, N - \sum A_k)}{N} - 1$.

Proof. Since $Q_\infty \in \pi^{-1}(\{P_\infty\})$ is not singular points of $\widetilde{C}$, and therefore $\widetilde{\pi}^* \omega_{(s,\boldsymbol{a})}$ is an element of $\Omega[\widetilde{C}]_{Q_\infty}$ if and only if $\widetilde{\pi}^* \omega_{(s,\boldsymbol{a})}$ is regular at Q_∞. By using Proposition 3.5 and Lemma 4.2, the proof of the theorem is completed. □

Let μ_N be the subgroup of $\overline{K}^\times$ consisting of N-th roots of unity as in previous sections. As with the case of $\Omega[C]$ in Section 4, the automorphism $(x, y) \mapsto (x, \zeta y)$ for $\zeta \in \mu_N$ induces an action of μ_N on $\Omega[\widetilde{C}]$. Let $\widetilde{W_s}$ be the subspace of $\Omega[\widetilde{C}]$ consisting of $\omega \in \Omega[\widetilde{C}]$ on which μ_N acts by $\omega \mapsto \zeta^s \omega$ for all $\zeta \in \mu_N$.

Corollary 5.3. For $0 \leq s \leq N - 1$, the set of $\omega_{s,j}$ with

$$\omega_{s,j} := \frac{x^{j-1} dx}{y^s}, \quad 1 \leq j \leq \frac{s \sum A_k - (N, N - \sum A_k)}{N} \tag{5.1}$$

is a basis of $\widetilde{W}_s$. In particular, we have

$$\dim \widetilde{W}_s = \max\left\{0, \left\lfloor \frac{s\sum A_k - (N, N - \sum A_k)}{N} \right\rfloor\right\}.$$

Proof. By Theorem 5.2, the differential forms $\omega_{s,j}$ in (5.1) belong to $\widetilde{W}_s$ and they are linearly independent obviously. Let $n = \sum A_k$ and $\mathcal{H}$ be the family

$$y^N = \prod_{j=0}^{r} \prod_{k=1}^{A_j} (x - \gamma_{jk}),$$

where $(\gamma_{jk}) \in \mathbb{A}^n$. Let $\widetilde{\mathcal{H}}$ be the family over $\mathbb{A}^n$ obtained as the fiberwise desingularization only at ∞ of $\mathcal{H}$. Note that $\Omega[\widetilde{C}]$ is the space of global sections of the dualizing sheaf of $\widetilde{C}$. By the similar way as in Corollary 4.6, the dimension of $\Omega[\widetilde{\mathcal{H}}]$ is equal to $\dim \Omega[\widetilde{\mathcal{H}}(t)]$ for a smooth fiber $\widetilde{\mathcal{H}}(t)$ with $t \in \mathbb{A}^n$ of $\widetilde{\mathcal{H}}$. Moreover $\dim \Omega[\widetilde{\mathcal{H}}(t)]$ is equal to the dimension which we have computed in Theorem 3.6 for $A_j = 1$ for $j = 1, \ldots, r$, which is

$$\sum_{s=0}^{N-1} \max\left\{0, \left\lfloor \frac{s\sum A_k - (N, N - \sum A_k)}{N} \right\rfloor\right\}.$$

This implies that $\{\omega_{s,j}\}$ has to span $\widetilde{W}_s$. □

Summarizing the discussions the above, we obtain the Main Theorem C in Section 1.

Example 5.4. We consider the curve $C : y^3 = x(x-1)^2(x-z)^2$ in Example 4.7. Then,

$$\left\{\frac{dx}{y}, \frac{dx}{y^2}, \frac{xdx}{y^2}, \frac{x^2dx}{y^2}\right\}$$

forms a basis of $\Omega[\widetilde{C}]$.

6. The modified Cartier operator on the regular differential module

In this section, we assume that K is a perfect field of positive characteristic $p > 0$ which does not divide N. Let C be the projective model of

$$y^N = x^{A_0}(x - \lambda_1)^{A_1} \cdots (x - \lambda_r)^{A_r} =: f(x),$$

i.e., a curve associated to Appell-Lauricella hypergeometric series as defined in Definition 2.1. We introduce the (modified) Cartier operator on the regular differential modules on X, C and $\widetilde{C}$, which were studied in the previous sections, and we describe the operator in terms of Appell-Lauricella hypergeometric series. Here, X is the desingularization of C, and $\widetilde{C}$ is the partial desingularization of C only at P_∞ (see Definition 5.1). Now, we start with recalling [24, Definition 2.1] the definition of the modified Cartier operator $\mathcal{C}'$ on the space $\Omega(C)$ of rational differential forms on C.

Definition 6.1. For all differential forms $\omega \in \Omega(C)$, there exist $\phi, \eta \in K(x, y)$ uniquely such that $\eta^p \in K(x^p, y^p)$ and

$$\omega = d\phi + \eta^p x^{p-1} dx.$$

Then, the modified Cartier operator $\mathcal{C}' : \Omega(C) \longrightarrow \Omega(C)$ is defined as $\mathcal{C}'(\omega) = \eta dx$.

It is well-known that the modified Cartier operator $\mathcal{C}'$ stabilizes $\Omega[X]$. The next theorem says that this also holds for $\Omega[C]$ and $\Omega[\widetilde{C}]$.

Theorem 6.2. The modified Cartier operator $\mathcal{C}'$ stabilizes $\Omega[C]$ and $\Omega[\tilde{C}]$. More generally, $\mathcal{C}'$ stabilizes $\Omega[C]_P$ for any closed point $P \in C$, where $\Omega[C]_P$ is as defined in (4.1).

Proof. It suffices to show the second assertion. Let $\omega \in \Omega[C]_P$. Let x_P be the x-coordinate of P. By replacing x by $x - x_P$, we may assume that x takes 0 at P. Note that the modified Cartier operator does not change by this replacement. Write

$$\omega = d\phi + \eta^p x^{p-1} dx. \tag{6.1}$$

Let h be an arbitrary element of $\mathcal{O}_{C,P}$. Multiplying (6.1) by $\pi^*(h^p)$, we get

$$\pi^*(h^p)\omega = d(\pi^*(h^p)\phi) + (\pi^*(h)\eta)^p x^{p-1} dx.$$

We have

$$\Big(\sum_{\pi(Q)=P} \mathrm{res}_Q(\pi^*(h)\eta dx)\Big)^p = \sum_{\pi(Q)=P} \mathrm{res}_Q((\pi^*(h)\eta)^p x^{p-1} dx) = \sum_{\pi(Q)=P} \mathrm{res}_Q(\pi^*(h^p)\omega).$$

The right hand side is zero since $\omega \in \Omega[C]_P$. Hence, we have

$$\sum_{\pi(Q)=P} \mathrm{res}_Q(\pi^*(h)\eta dx) = 0$$

and therefore $\mathcal{C}'(\omega) = \eta dx \in \Omega[C]_P$. □

Definition 6.3. The *Cartier-Manin matrix* A of X (resp. C, $\widetilde{C}$) with respect to a basis $\{\xi_i\}$ of $\Omega[X]$ (resp. $\Omega[C]$, $\Omega[\widetilde{C}]$) is given by $A = (a_{ij})$ with $\mathcal{C}'(\xi_j) = \sum_i a_{ij}^{1/p}\,\xi_i$.

In order to describe the Cartier-Manin matrix, it suffices to describe the modified Cartier operator $\mathcal{C}'$ on

$$\omega_{s,j} = \frac{x^{j-1}}{y^s}dx$$

for each $1 \leq s \leq N-1$, since our basis of the space of regular differential forms (obtained in the previous sections) is given by linear combinations of $\omega_{s,j}$. We shall see that it can be described in terms of the Appell-Lauricella hypergeometric series. Now, recall that $p \nmid N$. Hence, there uniquely exist integers m'_s, n'_s with $1 \leq m'_s \leq N-1,\ 0 \leq n'_s < p$ such that

$$m'_s\, p - n'_s N = s$$

for $1 \leq s \leq N-1$ by Lemma A.6. We rewrite $\omega_{s,j}$ as

$$\omega_{s,j} = y^{-s}x^{j-1}dx = y^{-m'_s p}x^{j-1}y^{m'_s p-s}dx = \left(y^{m'_s}\right)^{-p}x^{j-1}f(x)^{n'_s}dx.$$

Let $\gamma_{s,e}$ be the coefficient of x^e in the polynomial $f(x)^{n'_s}$, namely

$$f(x)^{n'_s} = \sum_{e=0}^{n'_s \deg(f)} \gamma_{s,e}x^e.$$

Now we have

$$\begin{aligned}\omega_{s,j} &= (y^{m'_s})^{-p}\sum_{j+e\not\equiv 0\,(\mathrm{mod}\,p)}\gamma_{s,e}x^{j+e-1}dx + \sum_l \gamma_{s,(l+1)p-j}\frac{x^{(l+1)p}}{y^{m'_s p}}\frac{dx}{x}\\ &= d\left(y^{-m'_s p}\sum_{j+e\not\equiv 0\,(\mathrm{mod}\,p)}\frac{\gamma_{s,e}x^{j+e}}{j+e}\right) + \sum_l \gamma_{s,(l+1)p-j}\frac{x^{lp}}{y^{m'_s p}}x^{p-1}dx,\end{aligned}$$

where l runs from $\left\lceil \dfrac{j}{p} - 1\right\rceil$ to $\left\lfloor \dfrac{n'_s \deg(f) + j}{p} - 1\right\rfloor$.

Our final aim in this paper is to show Main Theorem D. As with elliptic curves, we also need to introduce a truncation of Appell-Lauricella hypergeometric series. Here, we let $\mathcal{F}(a, b_2, \dots, b_r, c\,; \lambda_2, \dots, \lambda_r)$ be the Appell-Lauricella hypergeometric series associated to the curve $C : y^N = x^{A_0}(x-1)^{A_1}\prod_{k=2}^r(x-\lambda_k)^{A_k}$, namely

$$a = -1 + \sum_{k=0}^{r}(A_k/N), \quad b_i = A_i/N, \quad c = a + 1 - (A_1/N),$$

as mentioned after Definition 2.3.

Definition 6.4 (The truncation of Appell-Lauricella hypergeometrix series)**.** For $(\sigma,\tau_1,\dots,\tau_r)\in\mathbb{Z}^{r+1}$, we let $\mathcal{F}^{(\sigma;\,\tau_1,\dots,\tau_r)}(a,b_2,\dots,b_r,c\,;\lambda_2,\dots,\lambda_r)$ be the polynomial defined by the sum of the $\lambda_2^{e_2}\cdots\lambda_r^{e_r}$-terms of $\mathcal{F}(a,b_2,\dots,b_r,c\,;\lambda_2,\dots,\lambda_r)$ for $(e_2,\dots,e_r)$ satisfying $e_j\le\tau_j$ for $j=2,\dots,r$ and

$$\sigma-\tau_1\le\sum_{k=2}^{r}e_k\le\sigma.$$

We call this polynomial *the truncation of* $\mathcal{F}(a,b_2,\dots,b_r,c\,;\lambda_2,\dots,\lambda_r)$ *with respect to* $(\sigma;\,\tau_1,\dots,\tau_r)$.

Unfortunately, it is *not* true in general that one can describe $\mathcal{C}'$ in terms of the Appell-Lauricella hypergeometric series $\mathcal{F}(a,b_2,\dots,b_r,c\,;\lambda_2,\dots,\lambda_r)$ itself of C. We will see that $\mathcal{C}'$ can be described in terms of Appell-Lauricella hypergeometric series associated to a deformation of $f(x)$ which is separable except for the factor of x, see $f_0(x)$ in (6.2) below for the explicit form. The description is as follows:

Theorem 6.5. Let a' be a positive rational number with $a'\equiv s\deg(f)/N-j$ (mod p) and set $c'=a'+1-s/N$ and $d'=n'_s\deg(f)-(l+1)p+j$. For $\lceil\frac{j}{p}-1\rceil\le l\le\lfloor\frac{n'_s\deg(f)+j}{p}-1\rfloor$, we have that $\gamma_{s,(l+1)p-j}$ is equal to

$$\frac{(c';d')}{(a';d')}\mathcal{F}^{(d';\,n'_s,\dots,n'_s)}(a',\underbrace{s/N,\dots,s/N}_{-1+\sum_{k\ge1}A_k},c';\underbrace{1,\dots,1}_{A_1-1},\underbrace{\lambda_2,\dots,\lambda_2}_{A_2},\dots,\underbrace{\lambda_r,\dots,\lambda_r}_{A_r}),$$

where the right hand side (a priori belonging to $\mathbb{Q}[\lambda_2,\dots,\lambda_r]$) is considered as a polynomial over $\mathbb{F}_p$ (note that the denominator of any coefficient is coprime to p).

First, we see that it is enough to show the case of $A_1=A_2=\cdots=A_r=1$.

Reduction to the case of $A_k=1$ *for* $k=1,\dots,r$. Consider

$$f_0(x)=x^{A_0}(x-1)\prod_{t=2}^{A_1}(x-\lambda_{1t})\prod_{k=2}^{r}\prod_{t=1}^{A_k}(x-\lambda_{kt}).\tag{6.2}$$

Write

$$f_0(x)^{n'_s}=\sum_c(\delta_0)_{s,c}x^c.$$

Then

$$\gamma_{s,c}=(\delta_0)_{s,c}|_{\lambda_{kt}=\lambda_k\text{for }k=1,\dots,r\text{and }t=1,\dots,A_k,\,(k,t)\neq(1,1)}\tag{6.3}$$

with $\lambda_1 = 1$ holds. We shall see in Proposition 6.7 below that $(\delta_0)_{s,(l+1)p-j}$ is equal to

$$\mathcal{F}^{(d';n'_s,\dots,n'_s)}(a', \underbrace{s/N, \dots, s/N}_{-1+\sum_{k\geq 1} A_k}, c'; \lambda_{12}, \dots, \lambda_{1A_1}, \lambda_{21}, \dots, \lambda_{2A_2}, \dots, \lambda_{r1}, \dots, \lambda_{rA_r}) \tag{6.4}$$

multiplied by $\frac{(c';d')}{(a';d')}$, which is the result in the case of $A_1 = A_2 = \cdots = A_r = 1$. Then, the theorem follows from equations (6.3) and (6.4). □

Lemma 6.6. Let a' be a positive rational number with $a' \equiv s\deg(f)/N - j \pmod p$ and set $c' = a' + 1 - sA_1/N$ and $d' = n'_s \deg(f) - (l+1)p + j$. For a partition $(d_1, \dots, d_r)$ of d' (i.e., $d' = \sum_{k=1}^{r} d_k$) with $0 \leq d_k < p$, the following is true:

$$(-1)^{d_k}\binom{n'_s A_k}{d_k} = (-1)^{d_k}\binom{-sA_k/N}{d_k} = \frac{(sA_k/N\,;d_k)}{(1\,;d_k)}$$

in $\mathbb{F}_p$ for $k = 1, \dots, r$. Moreover for $k = 1$, we have

$$(-1)^{d_1}\binom{n'_s A_1}{d_1} = \frac{(c';d')}{(a';d')}\frac{(a';d'-d_1)}{(c';d'-d_1)}$$

in $\mathbb{F}_p$.

Proof. Recall that $m'_s p - n'_s N = s$, then we have $n'_s = -s/N$ in $\mathbb{F}_p$. Hence $\binom{n'_s A_k}{d_k} = \binom{-sA_k/N}{d_k}$ for $k = 1, \dots, r$. The first equality follows from

$$\begin{aligned}(-1)^{d_k}\binom{-sA_k/N}{d_k} &= (-1)^{d_k}\frac{-sA_k/N(-sA_k/N-1)\cdots(-sA_k/N-d_k+1)}{d_k!}\\ &= \frac{(sA_k/N)(sA_k/N+1)\cdots(sA_k/N+d_k-1)}{d_k!} = \frac{(sA_k/N\,;d_k)}{(1\,;d_k)}\end{aligned}$$

for $k = 1, \dots, r$.

We prove the second equation by induction on d_1. If $d_1 = 0$, then the both sides are equal to one. Assume that the equation holds for smaller d_1. Then

$$(-1)^{d_1}\binom{n'_s A_1}{d_1} = -\frac{n'_s A_1 - d_1 + 1}{d_1}\cdot(-1)^{d_1-1}\binom{n'_s A_1}{d_1 - 1}$$

and

$$\frac{(c';d')}{(a';d')}\frac{(a';d'-d_1)}{(c';d'-d_1)} = \frac{c'+d'-d_1}{a'+d'-d_1}\cdot\frac{(c';d')}{(a';d')}\frac{(a';d'-(d_1-1))}{(c';d'-(d_1-1))}.$$

Then the equality for d_1 follows from that

$$a' + d' - d_1 = (s/N + n'_s)(\deg f) - d_1 = -d_1$$

in $\mathbb{F}_p$ and that by $c' = a' + 1 - sA_1/N$ we have

$$c' + d' - d_1 = -d_1 + 1 - sA_1/N = {n'}_s A_1 - d_1 + 1$$

in $\mathbb{F}_p$. □

Proposition 6.7. Assume that $A_k = 1$ for all $k = 1, \ldots, r$. We let a' be a positive rational number with $a' \equiv s \deg(f)/N - j \pmod p$. Set ${b'}_k = sb_k$ and $c' = a' + 1 - s/N$. Moreover, set $d' = {n'}_s \deg(f) - (l+1)p + j$. Consider a polynomial in $\lambda_2, \ldots, \lambda_r$ over $\mathbb{Q}$

$$\delta_{s,(l+1)p-j} := \frac{(c'; d')}{(a'; d')} \mathcal{F}^{(d'; \tau_1, \ldots, \tau_r)}(a', b'_2, \ldots, b'_r, c'; \lambda_2, \ldots, \lambda_r),$$

where $\tau_k := {n'}_s$ for all $k = 1, \ldots, r$. Then, we have the following statements:

(1) The denominator of every coefficient of $\delta_{s,(l+1)p-j}$ is coprime to p. Hence we can consider it as a polynomial over $\mathbb{F}_p$, say $\overline{\delta}_{s,(l+1)p-j}$.

(2) We have the equality $\gamma_{s,(l+1)p-j} = \overline{\delta}_{s,(l+1)p-j}$.

Remark 6.8. Setting ${a'}_0 := s \deg(f)/N - j$ and ${c'}_0 := s(\deg(f) - 1)/N - j + 1$, the Appell-Lauricella hypergeometric series $\mathcal{F}({a'}_0, {b'}_2, \ldots, {b'}_r, {c'}_0\,; \lambda_2, \ldots, \lambda_r)$ is associated to

$$\frac{x^{j-1}}{y^s} dx = \frac{1}{x^{sA_0/N - j + 1}(x-1)^{sA_1/N}(x-\lambda_2)^{sA_2/N} \cdots (x-\lambda_r)^{sA_r/N}}$$

with $A_1 = A_2 = \cdots = A_r = 1$. Indeed, we have

$$\begin{aligned} {a'}_0 &= -1 + (sA_0/N - j + 1) + \sum_{k=1}^{r} (sA_k/N) \\ &= s\Big(-1 + \sum_{k=0}^{r} (A_k/N)\Big) - j + s = sa - j + s \end{aligned}$$

and

$${c'}_0 = {a'}_0 + 1 - (sA_1/N) = s(a - A_1/N + 1) - j + 1 = sc - j + 1.$$

In the theorem, we use a positive a' instead of possibly non-positive a'_0 so that $(a'; d')$ ($\in \mathbb{Q}$) and the denominators ($\in \mathbb{Q}$) of coefficients of the hypergeometric series are not zero.

Proof of Proposition 6.7. Assume that $A_k = 1$ for $k = 1, \ldots, r$. Then

$$f(x) = x^{A_0}(x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_r)$$

with $\lambda_1 = 1$, and $f(x)^{n'_s}$ is computed as

$$\begin{aligned} f(x)^{n'_s} &= x^{n'_s A_0}(x-\lambda_1)^{n'_s}\cdots(x-\lambda_r)^{n'_s} \\ &= x^{n'_s A_0}\prod_{k=1}^{r}\sum_{d_k=1}^{n'_s}\binom{n'_s}{d_k}(-1)^{d_k}\lambda^{d_k}x^{n'_s-d_k} \\ &= \sum_{d_1,\dots,d_k}\prod_{k=1}^{r}(-1)^{d_k}\binom{n'_s}{d_k}\lambda_1^{d_1}\cdots\lambda_r^{d_r}x^{n'_s\deg(f)-(d_1+\cdots+d_r)}. \end{aligned}$$

The $x^{(l+1)p-j}$-coefficient $\delta_{s,(l+1)p-j}$ of $f(x)^{n'_s}$ is

$$\sum_{d_1,\dots,d_k}\prod_{k=1}^{r}(-1)^{d_k}\binom{n'_s}{d_k}\lambda_1^{d_1}\cdots\lambda_r^{d_r},$$

where $(d_1,\dots,d_r)$ runs the set of $(d_1,\dots,d_r)$ satisfying $0\le d_k\le n'_s$ and

$$d_1+\cdots+d_r = n'_s\deg(f)-(l+1)p-j = d'.$$

By Lemma 6.6, this is equal to

$$\frac{(c';d')}{(a';d')}\sum_{d_1,\dots,d_k}\frac{(a'\,;\sum_{k=2}^{r}d_k)}{(c'\,;\sum_{k=2}^{r}d_k)}\prod_{k=2}^{r}\frac{(s/N;d_k)}{(1;d_k)}\lambda_1^{d_1}\cdots\lambda_r^{d_r},$$

which is equal to

$$\frac{(c';d')}{(a';d')}\mathcal{F}^{(d'\,;\,n'_s,\dots,n'_s)}(a',b'_2,\dots,b'_r,c';\lambda_2,\dots,\lambda_r)$$

by $\lambda_1 = 1$. Thus the proposition was proved. □

We have described the modified Cartier operator $\mathcal{C}'$ on $\omega_{s,j} = \dfrac{x^{j-1}}{y^s}dx$. If we want to describe it on other elements for example $\omega_{(s,\boldsymbol{a})} := \dfrac{\prod_{i=0}^{r}(x-\lambda_i)^{a_i}}{y^s}dx$, we first write it as a linear combination of $\omega_{s,j}$, use the formula of $\mathcal{C}'$ on $\omega_{s,j}$ and rewrite the obtained image as a linear combination of $\omega_{(s,\boldsymbol{a})}$. Summarizing the discussions the above, we obtain the Main Theorem D in Section 1. In Theorem 6.5, we have shown that $\Omega[C]$ and $\Omega[\widetilde{C}]$ are closed under $\mathcal{C}'$. We can show more as for the subspaces W_s (resp. $\widetilde{W_s}$) of $\Omega[C]$ (resp. $\Omega[\widetilde{C}]$).

Theorem 6.9. The following statements are true:

(1) The modified Cartier operator $\mathcal{C}'$ on $\Omega[C]$ sends W_s to $W_{m'_s}$. Moreover in *Case 1*,

$$\mathcal{C}'\omega_{s,j} = \sum_{l=0}^{m'_s-2}\gamma_{s,(l+1)p-j}^{1/p}\cdot\omega_{m'_s,\,l+1}.$$

(2) The modified Cartier operator $\mathcal{C}'$ on $\Omega[\widetilde{C}]$ sends $\widetilde{W}_s$ to $\widetilde{W}_{m'_s}$. Moreover,

$$\mathcal{C}'\omega_{s,j} = \sum_{l=0}^{(m'_s \deg(f)-(N,\deg(f))/N-1} \gamma_{s,(l+1)p-j}^{1/p} \cdot \omega_{m'_s,l+1}.$$

Proof. First of all, note that $\mathcal{C}'$ sends $\omega_{s,j}$ to $\sum_l \gamma_{s,(l+1)p-j}^{1/p} \frac{x^l}{y^{m'_s}}dx$, where l runs between $\lceil \frac{j}{p} - 1 \rceil$ and $\lfloor \frac{n'_s \deg(f)+j}{p} - 1 \rfloor$. Hence, the space of the character $\zeta \mapsto \zeta^s$ for each $\zeta \in \mu_N$ is sent by $\mathcal{C}'$ to that of the character $\zeta \mapsto \zeta^{m'_s}$.

(1) Recall from Corollary 4.6 that $\omega_{s,j} = x^{j-1}dx/y^s$ for $0 \leq s < N$ and $1 \leq j < s$ give a basis of $\Omega[C]$. We have to show $l+1 < m'_s$. This follows from

$$l+1 \leq \left\lfloor \frac{n'_s \deg(f)+j}{p} \right\rfloor \leq \left\lfloor \frac{n'_s N + s - 1}{p} \right\rfloor \leq \left\lfloor \frac{m'_s p - 1}{p} \right\rfloor < m'_s.$$

(2) The set of $\widetilde{\pi}^*\omega_{s,j}$ with

$$\omega_{s,j} = \frac{x^{j-1}dx}{y^s}, \quad 1 \leq s \leq N-1,\ 1 \leq j \leq \frac{s\deg(f) - (N, N - \sum A_k)}{N}$$

is a basis of $\Omega[\widetilde{C}]$ by Corollary 5.3. By Corollary 5.3, we need to show that

$$1 \leq m'_s \leq N-1, \quad 1 \leq l+1 \leq \frac{m'_s \sum A_k - (N, N - \sum A_k)}{N}.$$

The former is clear. In addition $m'_s p - n'_s N = s$ and $jN \leq s\sum A_k - (N, N - \sum A_k)$, then we have

$$\left\lfloor \frac{n'_s \sum A_k + j}{p} \right\rfloor \leq \left\lfloor \frac{m'_s \sum A_k - (N, N - \sum A_k)}{N} + \frac{(N, N - \sum A_k)}{N}\frac{p-1}{p} \right\rfloor.$$

Rewriting the first term of right side as the irreducible fraction, the denominator is a divisor of $N/(N, N - \sum A_k)$, while the second term is strictly smaller than $(N, N - \sum A_k)/N$. Hence we obtain

$$\left\lfloor \frac{n'_s \sum A_k + j}{p} \right\rfloor \leq \frac{m'_s \sum A_k - (N, N - \sum A_k)}{N}.$$

This is the desired conclusion. □

In the last of this section, we give some examples:

Example 6.10. We consider the case C is a (nonsingular) hyperelliptic curve of genus $g \geq 1$. Write $C : y^2 = f(x) := x(x-1)(x-\lambda_2)\cdots(x-\lambda_{2g})$ with separable $f(x)$. Let us describe the modified Cartier operator on $\Omega[\widetilde{C}]$. By using Corollary

5.3, a basis is given by $x^{j-1}dx/y$ for $j = 1, \dots, g$. Note that $a = g-1/2$, $b_i = 1/2$ and $c = g$. We get $m'_1 = 1, n'_1 = (p-1)/2$. Put $a' = (2g+1)/2-j = g+1/2-j$ and $c' = g-j+1$, then these number are positive, and set $d' = \frac{p-1}{2}\deg(f)-ip+j$. Then we have $\gamma_{1,ip-j}$ is equal to

$$\frac{(p(2g-2i+1)-1)!!}{(p(2g-2i+1)-2)!!}\frac{(2g-2j-1)!!}{(2g-2j)!!}\mathcal{F}^{(d';n'_1,\dots,n'_1)}(a',1/2,\dots,1/2,c';\lambda_2,\dots,\lambda_{2g})$$

for each i, j. For example, for $(g,p) = (2,3)$ with $f(x) = x(x-1)(x-z_1)(x-z_2)(x-z_3)$, the Cartier-Manin matrix $(\gamma_{1,ip-j})$ is

$$\begin{pmatrix} 2z_1z_2z_3 + 2z_1z_2 + 2z_1z_3 + 2z_2z_3 & z_1z_2z_3 \\ 1 & 2z_1 + 2z_2 + 2z_3 + 2 \end{pmatrix}.$$

The series $\mathcal{F}(5/2-j, 1/2, 1/2, 1/2, 3-j; z_1, z_2, z_3)$ truncated by z_k-degree ≤ 1 with coefficients in $\mathbb{Q}$ is

$$\begin{aligned} &1 + \frac{3}{8}(z_1+z_2+z_3) + \frac{5}{32}(z_1z_2+z_1z_3+z_2z_3) + \frac{35}{512}z_1z_2z_3\text{for } j = 1, \\ &1 + \frac{1}{4}(z_1+z_2+z_3) + \frac{3}{32}(z_1z_2+z_1z_3+z_2z_3) + \frac{5}{128}z_1z_2z_3\text{for } j = 2. \end{aligned}$$

For further truncations, use $d' = 5-3i+j$ and $n'_1 = 1$ with Definition 6.4.

Example 6.11. We consider the curve $C : y^3 = x(x-1)^2(x-z)^2$ in Examples 4.7 and 5.4, i.e., $(A_0, A_1, A_2) = (1, 2, 2)$ and $N = 3$. Let us describe the Cartier operator on $\mathit{\Omega}[\widetilde{C}]$. Recall from Example 5.4 that a basis is given by $\frac{x^{j-1}}{y^s}dx$ for $(s, j) = (1, 1), (2, 1), (2, 2), (2, 3)$.

- If $p \equiv 1 \pmod 3$, we have $m'_s = s$ and $n'_s = (p-1)s/3$.
- If $p \equiv 2 \pmod 3$, we have $m'_1 = 2, n'_1 = (2p-1)/3, m'_2 = 1$ and $n'_2 = (p-2)/3$.

Put $a' = 5s/3-j$ and $c' = 4s/3-j+1$, which are positive and set $d' = 5n'_s-ip+j$. Then

$$\gamma_{s,ip-j} = \frac{(c';d')}{(a';d')}\mathcal{F}^{(d';n'_s,n'_s,n'_s,n'_s)}(a', s/3, s/3, s/3, c'; 1, z, z)$$

for $i = 1$ if $m'_s = 1$ and $i = 1, 2, 3$ if $m'_s = 2$. For example for $p = 7$, then the Cartier-Manin matrix M of $\widetilde{C}$ with respect to $\{\omega_{1,1}, \omega_{2,1}, \omega_{2,2}, \omega_{2,3}\}$ is given by

$$\begin{pmatrix} (z-1)^2(z^2+4z+1) & 0 & 0 & 0 \\ 0 & z^7 & -z^8-z^7 & z^8 \\ 0 & -z^7-1 & z^8+z^7+z+1 & -z^8-z \\ 0 & 1 & -z-1 & z \end{pmatrix}.$$

This implies that the a-number of $\widetilde{C}$ is 3 or 2 depending on whether z^2+4z+1 is zero or not, since $z \neq 1$. Here, the a-number of $\widetilde{C}$ is defined to be $\dim \Omega[\widetilde{C}] - \mathrm{rank}(M)$. For example for $p=5$, then the Cartier-Manin matrix M of $\widetilde{C}$ is given by

$$\begin{pmatrix} 0 & 3z+3 & z^2+4z+1 & 3z^2+3z \\ 4z^6+4z^5 & 0 & 0 & 0 \\ z^6+z^5+z+1 & 0 & 0 & 0 \\ 4z+4 & 0 & 0 & 0 \end{pmatrix}.$$

This implies that the a-number of $\widetilde{C}$ is 3 or 2 depending on whether z is -1 or not.

References

[1] Archinard, N.: *Hypergeometric Abelian Varieties*, Canad. J. Math. **55** (2003), 897–932.

[2] Bouw, I. I.: *The p-rank of ramified covers of curves*, Compos. Math. **126** (2001), 295–322.

[3] Brock, B. W.: *Superspecial curves of genera two and three*, Thesis (Ph. D.)–Princeton University (1993).

[4] Elkin, A.: *The rank of the Cartier operator on cyclic covers of the projective line*, J. Algebra **327** (2011), 1–12.

[5] González, J.: *Hasse-Witt matrices for the Fermat curves of prime degree*, Tôhoku Math. J. **49** (1997), 149–163.

[6] Gorenstein, D.: *An arithmetic theory of adjoint plane curves*, Trans. Amer. Math. Soc. **72** (1952), No. 3, 414–436.

[7] Hartshorne, R.: *Algebraic Geometry*, GTM **52**, Springer New York, 1977.

[8] Harvey, D. and Sutherland, A. V.: *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), Special Issue A, 257–273.

[9] Harvey, D. and Sutherland, A. V.: *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II*, Contemporary Mathematics **663** (2016), 127–148.

[10] Husemöller, D.: *Elliptic Curves*, GTM **111**. Springer New York, 1987.

[11] Ibukiyama, T., Katsura, T. and Oort, F.: *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), No. 2, 127–152.

[12] Igusa, J.: *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. U.S.A. **44** (1958), 312–314.

[13] Kudo, M. and Harashita, S.: *Superspecial curves of genus 4 in small characteristic*, Finite Fields and Their Applications **45** (2017), 131–169.

[14] Kudo, M., Harashita, S. and Senda, H.: *The existence of supersingular curves of genus 4 in arbitrary characteristic*, Research in Number Theory **6** (2020) , Article number: 44.

[15] Lang, S.: *Algebra*, GTM **211**, Springer New York, 2002.

[16] Manin, Yu. I.: *The theory of commutative formal groups over fields of finite characteristic*, Russian Mathematical Survey **18** (1963), 1–80.

[17] Ohashi, R., Kudo, M. and Harashita, S.: *The a-numbers of non-hyperelliptic curves of genus three with large cyclic automorphism group*, arXiv:2111.09777.

[18] Serre, J.-P.: *Algebraic Groups and Class Fields*, GTM **117**, Springer New York, 1988.

[19] Silverman, J. H.: *The Arithmetic of Elliptic Curves*, GTM **106**, Springer New York, 1986.

[20] Stöhr, K.-O. and Voloch, J. F.: *A formula for the Cartier operator on plane algebraic curves*, J. Reine Angew. Math. **377** (1987), 49–64.

[21] Sutherland, A. V.: *Counting points on superelliptic curves in average polynomial time*, Fourteenth Algorithmic Number Theory Symposium, The Open Book Series **4** (2020), 403–422.

[22] Varchenko, A.: *Hyperelliptic integrals modulo p and Cartier-Manin matrices*, Pure Appl. Math. Q. **16** (2020), No. 3, 315-336.

[23] Whittaker, E. T. and Watson, G. N.: *A Course of Modern Analysis*, Cambridge University Press, 1927.

[24] Yui, N.: *On the Jacobian varieties of hyperelliptic curves over fields of characteristic p* > 2, J. Algebra **52** (1978), No. 2, 378–410.

A. Results from elementary number theory

In this section, we prove some propositions used in Sections 4-6. Let p, q be co-prime positive integers. Let g be a natural number.

Lemma A.1. *Every integer d with $d \geq pq+1$ can be written as $d = pa+qb$ for some positive integers a, b.*

Proof. Let r be the remainder of $d \geq pq+1$ divided by q. Now each remainder of $p, 2p, \ldots, pq$ divided by q is different, and thus there exists $1 \leq a \leq q$ such that the remainder of pa divided by q is r. Since $d - pa$ is divided by q, then $d = pa + qb$, where b denotes its quotient. □

Lemma A.2. *Every integer d with $d \geq gpq+1$ can be written as $d = pa+qb$ for positive integers a, b in at least g ways.*

Proof. Since $d-(g-1)pq \geq pq+1$, we can write $d-(g-1)pq = pa+qb$ $(a, b \geq 1)$ by using Lemma A.1. Then we have $d = p(a+iq) + q(b-(i-g+1)p)$ where $i = 0, \ldots, g-1$. Here, note that $a+iq$, $b-(i-g+1)p \geq 1$ hold. □

Corollary A.3. *Every integer d with $d \geq gpq-p-q+1$ can be written as $d = pa+qb$ for integers $a, b \geq 0$ in at least g ways.*

Proof. If $d \geq gpq-p-q+1$, then $d+p+q \geq gpq+1$ is written as $d+p+q = pa+qb$ $(a, b \geq 1)$ in different g ways by Lemma A.2. Thus $d = p(a-1)+q(b-1)$, so the proposition is true. □

Proposition A.4. *Let m, n be integers satisfying $np + mq = 1$. Then the following are true:*

(1) *Let d be an integer with $d \geq gpq-p-q+1$. For any $e \in \{0, \ldots, g-1\}$,*

there exists a pair (a, b) of non-negative integers such that $d = pa + qb$ and $e \equiv -ma + nb \pmod g$.

(2) Let $d = gpq-p-q$. For any non-negative integers a, b satisfying $d = pa+qb$, then we have $-ma + nb \not\equiv m - n \pmod g$.

Proof. (1) Let a_0 and b_0 be positive integers with $d - (g-1)pq = pa_0 + qb_0$. Set $a_i := a_0 + iq$ and $b_i := b_0 + (g-1-i)p$ for each $i = 0, \dots, g-1$. Let e_i be the element of $\{0, \dots, g-1\}$ with $e_i \equiv -ma_i + nb_i \pmod g$. It suffices to show $e_i \not\equiv e_j \pmod g$ for $0 \le i < j \le g-1$. This follows from

$$e_i - e_j = (-ma_i + nb_i) - (-ma_j + nb_j) = -m(a_i - a_j) + n(b_i - b_j)$$
$$= -mq(i-j) - np(i-j) = -(np + mq)(i-j) = j - i \not\equiv 0 \pmod g.$$

(2) Let $a_0 = -1$ and $b_0 = p-1$, then $d-(g-1)pq = pa_0+qb_0$. Set $a_i := a_0+iq$ and $b_i := b_0+(g-1-i)p$ for each $i = 0, \dots, g$. Then any pair (a, b) of non-negative integers such that $d = pa+qb$ is given by (a_i, b_i) for an $i = 1, \dots, g-1$. Similarly as the proof of (1), let e_i be the element of $\{0, \dots, g-1\}$ with $e_i \equiv -ma_i + nb_i \pmod g$. It suffices to show that $e_i \not\equiv m - n \pmod g$ for $1 \le i \le g-1$. This follows from

$$\begin{aligned} e_i - (m-n) &= (-ma_i + nb_i) - (m-n) \\ &= -m(a_i + 1) + n(b_i + 1) = -m(a_i - a_0) + n(b_i - b_0 + p) \\ &= -mqi + np(g-i) \\ &= -npg - (np + mq)i = -npg - i \not\equiv 0 \pmod g. \end{aligned}$$

Hence, the proof is completed. □

The next proposition is a generalization of [16, Lemma 3.8], where Manin proved the case of $g = 1$. Put $d_0 = gpq - p - q$ and $e_0 = m - n$.

Proposition A.5. Let d be an integer such that $0 \le d \le gpq-p-q$, and e be an integer such that $0 \le e \le g-1$. Then, there does not exist a pair (a, b) of non-negative integers such that $d = pa+qb$ and $e \equiv -ma+nb \pmod g$ if and only if there exists a pair (a', b') of non-negative integers such that $d = d_0 - (pa' + qb')$ and $e \equiv e_0 - (-ma' + nb') \pmod g$.

Proof. First, we show the "if"-part by contradiction. Assume that there exists a pair (a', b') of non-negative integers such that $d = d_0 - (pa' + qb')$, $e \equiv e_0 - (-ma' + nb') \pmod g$ and there is a pair (a, b) of non-negative integers such that $d = pa + qb$, $e \equiv -ma + nb \pmod g$. Then $d_0 = p(a + a') + q(b + b')$ and $e_0 \equiv -m(a + a') + n(b + b') \pmod g$. This contradicts Proposition A.4 (2).

Next we show the “only if”-part. Assume that there does not exist a pair (a, b) of non-negative integers such that $d = pa+qb$ and $e \equiv -ma+nb \pmod{g}$. We claim that there exists a pair (a'', b'') with $0 \leq a'' \leq gq-1$, $b'' < 0$ such that $d = pa''+qb''$ and $e \equiv -ma''+nb'' \pmod{g}$. Let a''_0 be the smallest non-negative integer with $d \equiv pa''_0 \pmod{q}$ and let $b''_0 = (d-pa''_0)/q$. We choose k in $\{0, \ldots, g-1\}$ such that $e \equiv -ma''_0+nb''_0-k \pmod{g}$. We put $a'' = a''_0+qk$ and $b'' = b''_0-pk$. Then we have $d = pa''+qb''$ and $e \equiv -ma''+nb'' \pmod{g}$. By the assumption, we have $b'' < 0$. Thus the claim was proved. The (a'', b'') obtained in the claim satisfies

$$\begin{aligned} d_0 - d &= gpq-p-q-(pa''+qb'') = p(gq-1-a'')+q(-b''-1), \\ e_0 - e &\equiv -m(-a''-1)+n(-b''-1) \\ &\equiv -m(gq-1-a'')+n(-b''-1) \pmod{g}. \end{aligned}$$

Put $a' := gq-1-a''$ and $b' := -b''-1$, then a' and b' are non-negative integers and must satisfy $d = d_0-(pa'+qb')$ and $e \equiv e_0-(-ma'+nb') \pmod{g}$. □

Lemma A.6. Let p, q be co-prime positive integers and let d be an integer with $0 < d < q$ such that d can not be divided by p. Then, there uniquely exist a, b such that $d = pa-qb$ with $0 < a < q$, $0 < b < p$.

Proof. There exist $a_0, b_0 \in \mathbb{Z}$ such that $pa-qb = d$ by Lemma A.1, so $(a, b) = (a_0+qk, b_0+pk)$ satisfy $pa-qb = d$ for all $k \in \mathbb{Z}$. Since $a_0 \not\equiv 0 \pmod{q}$, we can choose k such that $0 < a < q$. Now $-d < qb < pq-d$, then $-d/q < b < p-(d/q)$ and note that $0 < d/q < 1$. □

Ryo Ohashi
Graduate School of Information Science and Technology,
The University of Tokyo,
7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-8656,
Japan.
E-mail: `ryo-ohashi@g.ecc.u-tokyo.ac.jp`

Shushi Harashita
Graduate School of Environment and Information Sciences,
Yokohama National University,
79-7 Tokiwadai, Hodogaya-ku, Yokohama, 240-8501,
Japan.
E-mail: `harasita@ynu.ac.jp`