

HYPERELLIPTIC INTEGRALS MODULO p AND CARTIER-MANIN MATRICES

ALEXANDER VARCHENKO

*Department of Mathematics, University of North Carolina at Chapel Hill
Chapel Hill, NC 27599-3250, USA*

*Faculty of Mathematics and Mechanics, Lomonosov Moscow State University
Leninskiye Gory 1, 119991 Moscow GSP-1, Russia*

Key words: KZ equations, hyperelliptic integrals, Cartier-Manin matrix, reduction to characteristic p

2010 Mathematics Subject Classification: 13A35 (33C60, 32G20)

ABSTRACT. The hypergeometric solutions of the KZ equations were constructed almost 30 years ago. The polynomial solutions of the KZ equations over the finite field \mathbb{F}_p with a prime number p of elements were constructed recently. In this paper we consider the example of the KZ equations whose hypergeometric solutions are given by hyperelliptic integrals of genus g . It is known that in this case the total $2g$ -dimensional space of holomorphic solutions is given by the hyperelliptic integrals. We show that the recent construction of the polynomial solutions over the field \mathbb{F}_p in this case gives only a g -dimensional space of solutions, that is, a "half" of what the complex analytic construction gives. We also show that all the constructed polynomial solutions over the field \mathbb{F}_p can be obtained by reduction modulo p of a single distinguished hypergeometric solution. The corresponding formulas involve the entries of the Cartier-Manin matrix of the hyperelliptic curve.

That situation is analogous to the example of the elliptic integral considered in the classical Y.I. Manin's paper in 1961.

CONTENTS

1. Introduction	2
2. KZ equations	2
2.1. Description of equations	2
2.2. Solutions of (2.2) over \mathbb{C}	3
2.3. Solutions of KZ equations (2.2) over \mathbb{F}_p	4
3. Linear independence of solutions $I^m(z)$	5
4. Binomial coefficients modulo p	6
4.1. Lucas's theorem	6
4.2. Useful identities	6
5. Solutions $J^m(z)$	7
5.1. Sets Δ_s^r	7
5.2. Definition	7
5.3. Formula for $J^m(z)$	8
6. Cartier-Manin matrix	10
7. Comparison of solutions over \mathbb{C} and \mathbb{F}_p	11
7.1. Distinguished holomorphic solution	11

7.2. Rescaling	12
7.3. Taylor expansion of $L(\lambda)$	12
7.4. Coefficients, nonzero modulo p	13
7.5. Decomposition of $L(\lambda)$ into the disjoint sum of polynomials	14
7.6. Distinguished solution over \mathbb{C} and solutions $J^m(z)$ over \mathbb{F}_p	15
References	16

1. INTRODUCTION

The hypergeometric solutions of the KZ equations were constructed almost 30 years ago, see [SV1, SV2]. The polynomial solutions of the KZ equations over the finite field \mathbb{F}_p with a prime number p of elements were constructed recently in [SV3]. In this paper we consider the example of the KZ equations whose hypergeometric solutions are given by hyperelliptic integrals of genus g . It is known that in this case the total $2g$ -dimensional space of holomorphic solutions is given by the hyperelliptic integrals. We show that the recent construction of the polynomial solutions over the field \mathbb{F}_p in this case gives only a g -dimensional space of solutions, that is, a "half" of what the complex analytic construction gives. We also show that all the constructed polynomial solutions over the field \mathbb{F}_p can be obtained by reduction modulo p of a single distinguished hypergeometric solution. The corresponding formulas involve the entries of the Cartier-Manin matrix of the hyperelliptic curve.

That situation is analogous to the example of the elliptic integral considered in the classical Y.I. Manin's paper in 1961.

The paper is organized as follows. In Section 2 we describe the KZ equations, and construct for them two types of solutions: over \mathbb{C} and over \mathbb{F}_p . In Section 3 we show that the solutions, constructed over \mathbb{F}_p , form a module, denoted by $\mathcal{M}_{g,p}$, of rank g . In Section 4 useful formulas on binomial coefficients are collected. In Section 5 a new basis of the module $\mathcal{M}_{g,p}$ is constructed. In Section 6 the Cartier-Manin matrix of a hyperelliptic curve is defined. In Section 7 we introduce a distinguished holomorphic solution of the KZ equations, reduce its Taylor expansion coefficients modulo p and express this reduction in terms of the polynomial solutions over \mathbb{F}_p and entries of the Cartier-Manin matrix.

The author thanks R. Arnold, F. Beukers, N. Katz, V. Schechtman, J. Stienstra, Y. Zarhin, and W. Zudilin for useful discussions. The author thanks MPI in Bonn for hospitality in May-June 2018 when this work had been finished.

2. KZ EQUATIONS

2.1. Description of equations. Let \mathfrak{g} be a simple Lie algebra over the field \mathbb{C} , $\Omega \in \mathfrak{g}^{\otimes 2}$ the Casimir element corresponding to an invariant scalar product on \mathfrak{g} , V_1, \dots, V_n finite-dimensional irreducible \mathfrak{g} -modules.

The system of KZ equations with parameter $\kappa \in \mathbb{C}^\times$ on a $\otimes_{i=1}^n V_i$ -valued function $I(z_1, \dots, z_n)$ is the system of the differential equations

$$(2.1) \quad \frac{\partial I}{\partial z_i} = \frac{1}{\kappa} \sum_{j \neq i} \frac{\Omega^{(i,j)}}{z_i - z_j} I, \quad i = 1, \dots, n,$$

where $\Omega^{(i,j)}$ is the Casimir element acting in the i -th and j -th factors, see [KZ, EFK]. The KZ differential equations commute with the action of \mathfrak{g} on $\otimes_{i=1}^n V_i$, in particular, they preserve the subspaces of singular vectors of given weight.

In [SV1, SV2] the KZ equations restricted to the subspace of singular vectors of given weight were identified with a suitable Gauss-Manin differential equations and the corresponding solutions of the KZ equations were presented as multidimensional hypergeometric integrals.

Let p be a prime number and \mathbb{F}_p the field with p elements. Let \mathfrak{g}^p be the same Lie algebra considered over \mathbb{F}_p . Let V_1^p, \dots, V_n^p be the \mathfrak{g}^p -modules which are reductions modulo p of V_1, \dots, V_n , respectively. If κ is an integer and p large enough with respect to κ , then one can look for solutions $I(z_1, \dots, z_n)$ of the KZ equations in $\otimes_{i=1}^n V_i^p \otimes \mathbb{F}_p[z_1, \dots, z_n]$. Such solutions were constructed in [SV3].

In this paper we address two questions:

- A. What is the number of independent solutions constructed in [SV3] for given \mathbb{F}_p ?
- B. How are those solutions related to the solutions over \mathbb{C} , that are given by hypergeometric integrals?

We answer these question in the example in which the hypergeometric solutions are presented by hyperelliptic integrals.

The object of our study is the following systems of equations. For a positive integer g and $z = (z_1, \dots, z_{2g+1}) \in \mathbb{C}^{2g+1}$, we study the column vectors $I(z) = (I_1(z), \dots, I_{2g+1}(z))$ satisfying the system of differential and algebraic linear equations:

$$(2.2) \quad \frac{\partial I}{\partial z_i} = \frac{1}{2} \sum_{j \neq i} \frac{\Omega^{(i,j)}}{z_i - z_j} I, \quad i = 1, \dots, 2g+1, \quad I_1(z) + \dots + I_{2g+1}(z) = 0,$$

where

$$\Omega^{(i,j)} = \begin{pmatrix} & & i & & j & & \\ & & \vdots & & \vdots & & \\ i \cdots & -1 & \cdots & 1 & \cdots & & \\ & & \vdots & & \vdots & & \\ j \cdots & 1 & \cdots & -1 & \cdots & & \\ & & \vdots & & \vdots & & \end{pmatrix},$$

and all other entries equal zero.

The system of equations (2.2) is the system of the KZ differential equations with parameter $\kappa = 2$ associated with the Lie algebra \mathfrak{sl}_2 and the subspace of singular vectors of weight $2g-1$ of the tensor power $(\mathbb{C}^2)^{\otimes(2g+1)}$ of two-dimensional irreducible \mathfrak{sl}_2 -modules, up to a gauge transformation, see this example in [V2, Section 1.1].

2.2. Solutions of (2.2) over \mathbb{C} . Consider the *master function*

$$(2.3) \quad \Phi(t, z_1, \dots, z_{2g+1}) = \prod_{a=1}^{2g+1} (t - z_a)^{-1/2}$$

and the $2g+1$ -vector of hyperelliptic integrals

$$(2.4) \quad I^{(\gamma)}(z) = (I_1(z), \dots, I_{2g+1}(z)),$$

where

$$(2.5) \quad I_j = \int \Phi(t, z_1, \dots, z_{2g+1}) \frac{dt}{t - z_j}, \quad j = 1, \dots, 2g + 1.$$

The integrals are over an element γ of the first homology group γ of the hyperelliptic curve with equation

$$y^2 = (t - z_1) \dots (t - z_{2g+1}).$$

Starting from such γ , chosen for given $\{z_1, \dots, z_{2g+1}\}$, the vector $I^{(\gamma)}(z)$ can be analytically continued as a multivalued holomorphic function of z to the complement in \mathbb{C}^n to the union of the diagonal hyperplanes $z_i = z_j$.

Theorem 2.1. *The vector $I^{(\gamma)}(z)$ satisfies the KZ equations (2.2).*

Theorem 2.1 is a classical statement probably known in the 19th century. Much more general algebraic and differential equations satisfied by analogous multidimensional hypergeometric integrals were considered in [SV1, SV2]. Theorem 2.1 is discussed as an example in [V2, Section 1.1].

Theorem 2.2 ([V1, Formula (1.3)]). *All solutions of the KZ equations (2.2) have this form. Namely, the complex vector space of solutions of the form (2.4) is $2g$ -dimensional.*

This theorem follows from the determinant formula for multidimensional hypergeometric integrals in [V1], in particular, from [V1, Formula (1.3)].

2.3. Solutions of KZ equations (2.2) over \mathbb{F}_p . We always assume that the prime number p satisfies the inequality

$$(2.6) \quad p \geq 2g + 1.$$

Define the *master polynomial*

$$(2.7) \quad \Phi_p(t, z_1, \dots, z_{2g+1}) = \prod_{a=1}^{2g+1} (t - z_a)^{(p-1)/2} \in \mathbb{F}_p[t, z]$$

and the $2g + 1$ -vector of polynomials

$$(2.8) \quad P(z) = (P_1(t, z), \dots, P_{2g+1}(t, z)), \quad P_j(t, z) = \frac{1}{t - z_j} \Phi_p(t, z_1, \dots, z_{2g+1}).$$

Consider the Taylor expansion

$$(2.9) \quad P(t, z) = \sum_{i=0}^{(p-1)/2 + gp - g - 1} P^i(z) t^i, \quad P^i(z) = (P_1^i(z), \dots, P_{2g+1}^i(z)),$$

with $P_j^i(z) \in \mathbb{F}_p[z]$.

Theorem 2.3 ([SV3]). *For every positive integer l , the vector $P^{lp-1}(z)$ satisfies the KZ equations (2.2).*

This statement is a particular case of [SV3, Theorem 2.4]. Cf. Theorem 2.3 with [K].

Theorem 2.3 gives exactly g solutions $P^{p-1}(z), \dots, P^{gp-1}(z)$. We denote

$$I^m(z) = (I_1^m(z), \dots, I_{2g+1}^m(z)),$$

where

$$(2.10) \quad I^m(z) := P^{(g-m)p-1}(z), \quad m = 0, \dots, g-1.$$

3. LINEAR INDEPENDENCE OF SOLUTIONS $I^m(z)$

Denote $\mathbb{F}_p[z^p] := \mathbb{F}_p[z_1^p, \dots, z_{2g+1}^p]$. The set of all solutions $I(z) \in \mathbb{F}_p[z]^{2g+1}$ of the KZ equations (2.2) is a module over the ring $\mathbb{F}_p[z^p]$ since equations (2.2) are linear and $\frac{\partial z_i^p}{\partial z_j} = 0$ in $\mathbb{F}_p[z]$ for all i, j . Denote by

$$\mathcal{M}_{g,p} = \left\{ \sum_{m=0}^{g-1} c_m(z) I^m(z) \mid c_m(z) \in \mathbb{F}_p[z^p] \right\},$$

the $\mathbb{F}_p[z^p]$ -module generated by $I^m(z)$, $m = 0, \dots, g-1$.

Theorem 3.1. *Let $p \geq 2g+1$. The solutions $I^m(z)$, $m = 0, \dots, g-1$, are linear independent over the ring $\mathbb{F}_p[z^p]$, that is, if $\sum_{m=0}^{g-1} c_m(z) I^m(z) = 0$ for some $c_m(z) \in \mathbb{F}_p[z^p]$, then $c_m(z) = 0$ for all m .*

Proof. For $m = 0, \dots, g-1$, the coordinates of the vector $I^m(z)$ are homogeneous polynomials in z of degree $(p-1)/2 + mp - g$ and

$$I_j^m(z) = \sum I_{j;\ell_1, \dots, \ell_{2g+1}}^m z_1^{\ell_1} \cdots z_{2g+1}^{\ell_{2g+1}},$$

where the sum is over the elements of the set

$$\Gamma_j^m = \left\{ (\ell_1, \dots, \ell_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g+1} \mid \sum_{i=1}^{2g+1} \ell_i = (p-1)/2 + mp - g, \right. \\ \left. 0 \leq \ell_j \leq (p-3)/2, \quad 0 \leq \ell_i \leq (p-1)/2 \text{ for } i \neq j \right\}$$

and

$$I_{j;\ell_1, \dots, \ell_{2g+1}}^m = (-1)^{(p-1)/2 + mp - g} \binom{(p-3)/2}{\ell_j} \prod_{i \neq j} \binom{(p-1)/2}{\ell_i} \in \mathbb{F}_p.$$

Notice that all coefficients $I_{j;\ell_1, \dots, \ell_{2g+1}}^m$ are nonzero. Hence each solution $I^m(z)$ is nonzero.

We show that already the first coordinates $I_1^m(z)$, $m = 0, \dots, g-1$, are linear independent over the ring $\mathbb{F}_p[z^p]$.

Let $\bar{\Gamma}_1^m \subset \mathbb{F}_p^{2g+1}$ be the image of the set Γ_1^m under the natural projection $\mathbb{Z}^{2g+1} \rightarrow \mathbb{F}_p^{2g+1}$. The points of $\bar{\Gamma}_1^m$ are in bijective correspondence with the points of Γ_1^m . Any two sets $\bar{\Gamma}_1^m$ and $\bar{\Gamma}_1^{m'}$ do not intersect, if $m \neq m'$. (The sets $\bar{\Gamma}_1^m$ are analogs in \mathbb{F}_p^{2g+1} of the Newton polytopes of the polynomials $I_1^m(z)$.)

For any m and any nonzero polynomial $c_m(z) \in \mathbb{F}_p[z_1^p, \dots, z_{2g+1}^p]$, consider the nonzero polynomial $c_m(z) I_1^m(z) \in \mathbb{F}_p[z_1, \dots, z_{2g+1}]$ and the set Γ_{1,c_m}^m of points $\ell \in \mathbb{Z}^{2g+1}$ such that the monomial $z_1^{\ell_1} \cdots z_{2g+1}^{\ell_{2g+1}}$ enters $c_m(z) I_1^m(z)$ with nonzero coefficient. Then the natural projection of Γ_{1,c_m}^m to \mathbb{F}_p^{2g+1} coincides with $\bar{\Gamma}_1^m$. Hence the polynomials $I_1^m(z)$, $m = 0, \dots, g-1$, are linear independent over the ring $\mathbb{F}_p[z^p]$. \square

4. BINOMIAL COEFFICIENTS MODULO p

In this section we collect useful formulas on binomial coefficients.

4.1. Lucas's theorem.

Theorem 4.1 ([L]). *For non-negative integers m and n and a prime p , the following congruence relation holds:*

$$(4.1) \quad \binom{m}{n} \equiv \prod_{i=0}^k \binom{m_i}{n_i} \pmod{p},$$

where $m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$ and $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$ are the base p expansions of m and n respectively. This uses the convention that $\binom{m}{n} = 0$ if $m < n$. \square

Lemma 4.2. *For $a \in \mathbb{Z}_{>0}$, we have*

$$\binom{2a}{a} \not\equiv 0 \pmod{p}$$

if and only if the base p expansion of $a = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$ has the property:

$$a_i \leq \frac{p-1}{2} \quad \text{for } i = 0, \dots, k.$$

In that case

$$(4.2) \quad \binom{2a}{a} \equiv \prod_{i=0}^k \binom{2a_i}{a_i} \pmod{p}.$$

The lemma is a corollary of Lucas's theorem.

4.2. Useful identities. For $0 \leq k \leq (p-3)/2$, we have

$$(4.3) \quad \begin{aligned} \binom{(p-3)/2}{k} &= \binom{(p-1)/2}{k} \frac{(p-3)/2 - k + 1}{(p-1)/2} = \binom{(p-1)/2}{k} \frac{p-2k-1}{p-1} \\ &\equiv \binom{(p-1)/2}{k} (2k+1) \pmod{p}, \end{aligned}$$

for $0 \leq k \leq (p-1)/2$

$$(4.4) \quad \begin{aligned} \binom{(p-3)/2}{k-1} &= \binom{(p-1)/2}{k} \frac{k}{(p-1)/2} = \binom{(p-1)/2}{k} \frac{2k}{p-1} \\ &\equiv \binom{(p-1)/2}{k} (-2k) \pmod{p}. \end{aligned}$$

For a positive integer k ,

$$\begin{aligned}
 (4.5) \quad \binom{-1/2}{k} &= \frac{(-1/2)(-1/2-1)\cdots(-1/2-(k-2))(-1/2-(k-1))}{k!} \\
 &= (-2)^{-k} \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)}{k!} = (-1)^k 2^{-k} \frac{(2k)! / (2 \cdot 4 \cdot 6 \cdot 8 \cdots \cdot 2k)}{k!} \\
 &= (-1)^k 2^{-k} \frac{(2k)! / (2^k k!)}{k!} = (-4)^k \binom{2k}{k},
 \end{aligned}$$

for $0 \leq k \leq (p-1)/2$

$$(4.6) \quad \binom{(p-1)/2}{k} \equiv (-4)^{-k} \binom{2k}{k} \pmod{p}.$$

5. SOLUTIONS $J^m(z)$

5.1. **Sets Δ_s^r .** We introduce sets that are used later. For $r = 0, \dots, g-1$, $s = 0, \dots, g$, define

$$(5.1) \quad \Delta_s^r = \{(\ell_3, \dots, \ell_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g-1} \mid 0 \leq \sum_{i=3}^{2g+1} \ell_i + s - rp \leq (p-1)/2, \ell_i \leq (p-1)/2\}.$$

5.2. **Definition.** Introduce the vectors $J^m(z) \in \mathbb{F}_p[z]^{2g+1}$, $m = 0, \dots, g-1$, by the formula

$$(5.2) \quad J^m(z) = \sum_{l=0}^m I^{m-l}(z) z_1^{lp} \binom{g-m-1+l}{g-m-1},$$

that is,

$$\begin{aligned}
 J^0(z) &= I^0(z), \\
 J^1(z) &= I^0(z) z_1^p \binom{g-1}{g-2} + I^1(z), \\
 J^2(z) &= I^0(z) z_1^{2p} \binom{g-1}{g-3} + I^1(z) z_1^p \binom{g-2}{g-3} + I^2(z),
 \end{aligned}$$

and so on.

Lemma 5.1. *For $m = 0, \dots, g-1$, the vector $J^m(z)$ is a solution of the KZ equations (2.2). Moreover, the $\mathbb{F}_p[z^p]$ -module spanned by $J^m(z)$, $m = 0, \dots, g-1$, coincides with the $\mathbb{F}_p[z^p]$ -module $\mathcal{M}_{g,p}$ spanned by $I^m(z)$, $m = 0, \dots, g-1$. \square*

For the vector $P(t, z)$ in (2.9), consider the Taylor expansion

$$(5.3) \quad P(t + z_1, z) = \sum_{i=0}^{(p-1)/2 + gp - g - 1} \tilde{P}^i(z) t^i.$$

Lemma 5.2. *For $m = 0, \dots, g-1$, we have*

$$(5.4) \quad J^m(z) = \tilde{P}^{(g-m)p-1}(z),$$

cf. formula (2.10).

Proof. We have $P(t, z) = \sum_{i=0}^{(p-1)/2+gp-g-1} P^i(z)t^i$, hence

$$P(t + z_1, z) = \sum_{i=0}^{(p-1)/2+gp-g-1} P^i(z)(t + z_1)^i = \sum_{i=0}^{(p-1)/2+gp-g-1} P^i(z) \sum_{j=0}^i \binom{i}{j} t^j z_1^{i-j}.$$

If $p \nmid (i+1)$, then $\binom{i}{(m-g)p-1} \equiv 0 \pmod{p}$ by Lucas's theorem. Hence

$$\begin{aligned} \tilde{P}^{(g-m)p-1}(z) &= P^{(g-m)p-1}(z) \binom{(g-m)p-1}{(g-m)p-1} + P^{(g-m+1)p-1}(z) z_1^p \binom{(g-m+1)p-1}{(g-m)p-1} \\ &\quad + P^{(g-m+2)p-1}(z) z_1^{2p} \binom{(g-m+2)p-1}{(g-m)p-1} + \dots \\ &= I^m(z) + I^{m-1}(z) z_1^p \binom{g-m}{g-m-1} + I^{m-2}(z) z_1^{2p} \binom{g-m+1}{g-m-1} + \dots, \end{aligned}$$

where the last equality holds also by Lucas's theorem. This gives the lemma. \square

5.3. Formula for $J^m(z)$. Denote

$$(5.5) \quad \lambda_j = \frac{z_j - z_1}{z_2 - z_1}, \quad j = 1, \dots, 2g+1.$$

Theorem 5.3. For $m = 0, \dots, g-1$, we have

$$(5.6) \quad J^m(z) = (z_2 - z_1)^{(p-1)/2+mp-g} K^m(\lambda),$$

where

$$(5.7) \quad K^m(\lambda) = \sum_{\ell \in \Delta_g^m} K_\ell^m(\lambda),$$

Δ_j^m is defined in (5.1), and

$$(5.8) \quad \begin{aligned} K_\ell^m(\lambda) &= (-1)^{(p-1)/2+mp-g} \binom{(p-1)/2}{\sum_{i=3}^{2g+1} \ell_i + g - mp} \prod_{i=2}^{2g+1} \binom{(p-1)/2}{\ell_i} \lambda_s^{\ell_3} \dots \lambda_{2g+1}^{\ell_{2g+1}} \\ &\quad \times (1, -2 \sum_{i=3}^{2g+1} \ell_i - 2g, 2\ell_3 + 1, \dots, 2\ell_{2g+1} + 1). \end{aligned}$$

Using (4.6) we may rewrite formula (5.8) as

$$(5.9) \quad \begin{aligned} K_\ell^m(\lambda) &= (-1)^{(p-1)/2} 4^{-2 \sum_{i=3}^{2g+1} \ell_i - g + mp} \\ &\quad \times \binom{2 \sum_{i=3}^{2g+1} \ell_i + 2g - 2mp}{\sum_{i=3}^{2g+1} \ell_i + g - mp} \prod_{i=2}^{2g+1} \binom{2\ell_i}{\ell_i} \lambda_s^{\ell_3} \dots \lambda_{2g+1}^{\ell_{2g+1}} \\ &\quad \times (1, -2 \sum_{i=3}^{2g+1} \ell_i - 2g, 2\ell_3 + 1, \dots, 2\ell_{2g+1} + 1). \end{aligned}$$

Proof. We have

$$\begin{aligned} P((z_2 - z_1)x + z_1, z) &= (z_2 - z_1)^{(p-1)/2+gp-g-1} \\ &\quad \times x^{(p-1)/2} (x-1)^{(p-1)/2} \prod_{j=3}^{2g+1} (x - \lambda_j)^{(p-1)/2} \left(\frac{1}{x}, \frac{1}{x-1}, \frac{1}{x-\lambda_3}, \dots, \frac{1}{x-\lambda_{2g+1}} \right) \end{aligned}$$

and

$$P((z_2 - z_1)x + z_1, z) = \sum_{i=0}^{(p-1)/2+gp-g-1} \tilde{P}^i(z)(z_2 - z_1)^i x^i.$$

Hence $J^m(z) = \tilde{P}^{(g-m)p-1}(z)$ equals the coefficient of $x^{(g-m)p-1}$ in

$$(5.10) \quad x^{(p-1)/2}(x-1)^{(p-1)/2} \prod_{j=3}^{2g+1} (x - \lambda_j)^{(p-1)/2} \left(\frac{1}{x}, \frac{1}{x-1}, \frac{1}{x-\lambda_3}, \dots, \frac{1}{x-\lambda_{2g+1}} \right)$$

multiplied by $(z_2 - z_1)^{(p-1)/2+mp-g}$. We have

$$\begin{aligned} (z_2 - z_1)^{-(p-1)/2-mp+g} J_1^m(z) &= \\ (-1)^{(p-1)/2+mp-g} \sum \binom{(p-1)/2}{\ell_2} \cdots \binom{(p-1)/2}{\ell_{2g+1}} \lambda_3^{\ell_3} \cdots \lambda_{2g+1}^{\ell_{2g+1}}, \end{aligned}$$

where the sum is over the set

$$\begin{aligned} \Delta &= \{(\ell_2, \dots, \ell_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g} \mid \sum_{i=2}^{2g+1} \ell_i = mp - g + (p-1)/2, \\ &\quad \ell_j \leq (p-1)/2, j = 2, \dots, 2g+1\}. \end{aligned}$$

Expressing ℓ_2 from the conditions defining Δ we write

$$\begin{aligned} (z_2 - z_1)^{-(p-1)/2-mp+g} J_1^m(z) &= (-1)^{(p-1)/2+mp-g} \\ &\times \sum \binom{(p-1)/2}{\sum_{i=3}^{2g+1} \ell_i + g - mp} \binom{(p-1)/2}{\ell_3} \cdots \binom{(p-1)/2}{\ell_{2g+1}} \lambda_3^{\ell_3} \cdots \lambda_{2g+1}^{\ell_{2g+1}}, \end{aligned}$$

where the sum is over the set

$$\begin{aligned} \Delta_g^m &= \{(\ell_3, \dots, \ell_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g-1} \mid 0 \leq \sum_{i=3}^{2g+1} \ell_i + g - mp \leq (p-1)/2, \\ &\quad \ell_i \leq (p-1)/2, i = 3, \dots, 2g+1\}. \end{aligned}$$

Similarly we have

$$\begin{aligned} (z_2 - z_1)^{-(p-1)/2-mp+g} J_2^m(z) &= (-1)^{(p-1)/2+mp-g} \\ &\times \sum \binom{(p-3)/2}{\ell_2} \binom{(p-1)/2}{\ell_3} \cdots \binom{(p-1)/2}{\ell_{2g+1}} \lambda_3^{\ell_3} \cdots \lambda_{2g+1}^{\ell_{2g+1}}, \end{aligned}$$

where the sum is over the set

$$\begin{aligned} \Delta' &= \{(\ell_2, \dots, \ell_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g} \mid \sum_{i=2}^{2g+1} \ell_i = mp - g + (p-1)/2, \\ &\quad \ell_2 \leq (p-3)/2 \text{ and } \ell_i \leq (p-1)/2 \text{ for } i > 2\}. \end{aligned}$$

Expressing ℓ_2 from the conditions defining Δ' we write

$$\begin{aligned} (z_2 - z_1)^{-(p-1)/2-mp+g} J_2^m(z) &= (-1)^{(p-1)/2+mp-g} \\ &\times \sum \binom{(p-3)/2}{\sum_{i=3}^{2g+1} \ell_i + g - mp - 1} \binom{(p-1)/2}{\ell_3} \cdots \binom{(p-1)/2}{\ell_{2g+1}} \lambda_3^{\ell_3} \cdots \lambda_{2g+1}^{\ell_{2g+1}}, \end{aligned}$$

where the sum is over the set

$$\begin{aligned} \Delta'' &= \{(\ell_3, \dots, \ell_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g-1} \mid 0 \leq \sum_{i=3}^{2g+1} \ell_i + g - mp - 1 \leq (p-3)/2, \\ &\quad \ell_j \leq (p-1)/2, j = 3, \dots, 2g+1\}. \end{aligned}$$

For $j = 3, \dots, 2g+1$, we have

$$\begin{aligned} (z_2 - z_1)^{-(p-1)/2 - mp + g} J_j^m(z) &= (-1)^{(p-1)/2 + mp - g} \\ &\times \sum \binom{(p-3)/2}{\ell_j} \prod_{i=2, i \neq j}^{2g+1} \binom{(p-1)/2}{\ell_i} \lambda_3^{\ell_3} \cdots \lambda_{2g+1}^{\ell_{2g+1}}, \end{aligned}$$

where the sum is over the set

$$\begin{aligned} \Delta''' &= \{(\ell_2, \dots, \ell_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g} \mid \sum_{i=2}^{2g+1} \ell_i = mp - g + (p-1)/2, \\ &\quad \ell_j \leq (p-3)/2 \text{ and } \ell_i \leq (p-1)/2, i \neq j\}. \end{aligned}$$

Expressing ℓ_2 from the conditions defining Δ''' we write

$$\begin{aligned} (z_2 - z_1)^{-(p-1)/2 - mp + g} J_j^m(z) &= (-1)^{(p-1)/2 + mp - g} \\ &\times \sum \binom{(p-1)/2}{\sum_{i=3}^{2g+1} \ell_i + g - mp} \binom{(p-3)/2}{\ell_j} \prod_{i=2, i \neq j}^{2g+1} \binom{(p-1)/2}{\ell_i} \lambda_3^{\ell_3} \cdots \lambda_{2g+1}^{\ell_{2g+1}}, \end{aligned}$$

where the sum is over the set

$$\begin{aligned} \bar{\Delta}'''' &= \{(\ell_3, \dots, \ell_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g-1} \mid 0 \leq \sum_{i=3}^{2g+1} \ell_i + g - mp \leq (p-1)/2, \\ &\quad \ell_j \leq (p-3)/2 \text{ and } \ell_i \leq (p-1)/2, i \neq j\}. \end{aligned}$$

Using identities (4.3), (4.4) we may rewrite $J_j^m(z)$, $j = 2, \dots, 2g+1$, in the form indicated in the theorem. \square

6. CARTIER-MANIN MATRIX

Consider the hyperelliptic curve X with equation

$$y^2 = x(x-1)(x-\lambda_3) \cdots (x-\lambda_{2g+1}),$$

where $\lambda_3, \dots, \lambda_{2g+1} \in \mathbb{F}_p$, while, in the previous section, $\lambda_3, \dots, \lambda_{2g+1}$ were rational functions in z , see formula (5.5).

Following [AH] define the $g \times g$ Cartier-Manin matrix $C(\lambda) = (C_s^r(\lambda))_{s,r=0}^{g-1}$ of that curve. Namely, for $s = 0, \dots, g-1$, expand

$$x^{g-s-1} (x(x-1)(x-\lambda_3) \cdots (x-\lambda_{2g+1}))^{(p-1)/2} = \sum_k Q_s^k x^k$$

with $Q_j^k \in \mathbb{F}_p$ and set

$$(6.1) \quad C_s^r(\lambda) := Q_s^{(g-r)p-1}, \quad r = 0, \dots, g-1.$$

The Cartier-Manin matrix represents the action of the Cartier operator on the space of holomorphic differentials of the hyperelliptic curve. That operator is dual to the Frobenius operator on the cohomology group $H^1(X, \mathcal{O}_X)$, see for example, [AH].

Lemma 6.1. *We have*

$$(6.2) \quad C_s^r(\lambda) = \sum_{\ell \in \Delta_s^r} C_{s;\ell}^r(\lambda),$$

where Δ_s^r is defined in (5.1) and

$$(6.3) \quad C_{s;\ell}^r(\lambda) = (-1)^{(p-1)/2+rp-s} \binom{(p-1)/2}{\sum_{i=3}^{2g+1} \ell_i + s - rp} \prod_{i=3}^{2g+1} \binom{(p-1)/2}{\ell_i} \lambda_3^{\ell_3} \cdots \lambda_{2g+1}^{\ell_{2g+1}}.$$

□

The lemma is proved by straightforward calculation similar to the proof of Theorem 5.3. We may rewrite (6.3) as

$$(6.4) \quad C_{s;\ell}^r(\lambda) = (-1)^{(p-1)/2} 4^{-2 \sum_{i=3}^{2g+1} \ell_i - s + rp} \\ \times \binom{2 \sum_{i=3}^{2g+1} \ell_i + 2s - 2rp}{\sum_{i=3}^{2g+1} \ell_i + s - rp} \prod_{i=3}^{2g+1} \binom{2\ell_i}{\ell_i} \lambda_3^{\ell_3} \cdots \lambda_{2g+1}^{\ell_{2g+1}}.$$

7. COMPARISON OF SOLUTIONS OVER \mathbb{C} AND \mathbb{F}_p

Now we will

- (1) distinguish one holomorphic solution of the KZ equations,
- (2) expand it into the Taylor series,
- (3) for any $p \geq 2g + 1$ reduce this Taylor expansion modulo p ,
- (4) observe in that reduction of the Taylor expansion all polynomial solutions, that we have constructed and nothing more.

7.1. Distinguished holomorphic solution. Recall that holomorphic solutions of our KZ equations have the form $I(z) = (I_1(z), \dots, I_{2g+1}(z))$, where

$$I_j(z) = \int_{\gamma} \frac{dt}{\sqrt{(t-z_1) \cdots (t-z_{2g+1})}} \frac{1}{t-z_j}$$

and γ is an oriented curve on the hyperelliptic curve with equation $y^2 = (t-z_1) \cdots (t-z_{2g+1})$. Assume that z_3, \dots, z_{2g+1} are closer to z_1 than to z_2 :

$$\left| \frac{z_j - z_1}{z_2 - z_1} \right| < \frac{1}{2}, \quad j = 3, \dots, 2g + 1.$$

Choose γ to be the circle $\{t \in \mathbb{C} \mid \left| \frac{t-z_1}{z_2-z_1} \right| = \frac{1}{2}\}$ oriented counter-clockwise, and multiply the vector $I(z)$ by the normalization constant $1/2\pi$.

We call this solution $I(z)$ the *distinguished* solution.

7.2. Rescaling. Change variables and write

$$(7.1) \quad I(z_1, \dots, z_{2g+1}) = (z_2 - z_1)^{-1/2-g} L(\lambda_3, \dots, \lambda_{2g+1}),$$

where

$$(\lambda_3, \dots, \lambda_{2g+1}) = \left(\frac{z_3 - z_1}{z_2 - z_1}, \dots, \frac{z_{2g+1} - z_1}{z_2 - z_1} \right),$$

$$L(\lambda) = (L_1, \dots, L_{2g+1}),$$

$$L_j = \frac{-1}{2\pi} \int_{|x|=1/2} \frac{dx}{\sqrt{x(x-1)(x-\lambda_3) \dots (x-\lambda_{2g+1})}} \frac{1}{x-\lambda_j},$$

and we set $\frac{1}{x-\lambda_1} := \frac{1}{x}$, $\frac{1}{x-\lambda_2} := \frac{1}{x-1}$.

The function $L(\lambda)$ is holomorphic at the point $\lambda = 0$. Hence

$$L(\lambda) = \sum_{(k_3, \dots, k_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g-1}} L_{k_3, \dots, k_{2g+1}} \lambda_3^{k_3} \dots \lambda_{2g+1}^{k_{2g+1}},$$

where the coefficients lie in $\mathbb{Z}[\frac{1}{2}]^{2g+1}$. Hence for any $p \geq 2g+1$, this power series can be projected to a formal power series in $\mathbb{F}_p[\lambda]^{2g+1}$.

We relate this power series and the polynomial solutions $J^m(z)$, $m = 0, \dots, g-1$, constructed earlier.

7.3. Taylor expansion of $L(\lambda)$.

Lemma 7.1. *We have*

$$(7.2) \quad L(0, \dots, 0) = (-1)^g \binom{-1/2}{g} (1, -2g, 1, \dots, 1).$$

Proof. We have $\frac{-1}{2\pi} = \frac{(-1)^{-1/2}}{2\pi i}$ and

$$\begin{aligned} L_1(0, \dots, 0) &= \frac{(-1)^{-1/2}}{2\pi i} \int_{|x|=1/2} (x-1)^{-1/2} \frac{dx}{x^{g+1}} = \frac{1}{2\pi i} \int_{|x|=1/2} (1-x)^{-1/2} \frac{dx}{x^{g+1}} \\ &= \frac{1}{2\pi i} \int_{|x|=1/2} \sum_{k=0}^{\infty} (-1)^k x^k \binom{-1/2}{k} \frac{dx}{x^{g+1}} = (-1)^g \binom{-1/2}{g}, \end{aligned}$$

$$\begin{aligned} L_2(0, \dots, 0) &= \frac{(-1)^{-1/2}}{2\pi i} \int_{|x|=1/2} (x-1)^{-3/2} \frac{dx}{x^g} = -\frac{1}{2\pi i} \int_{|x|=1/2} (1-x)^{-3/2} \frac{dx}{x^g} \\ &= -\frac{1}{2\pi i} \int_{|x|=1/2} \sum_{k=0}^{\infty} (-1)^k x^k \binom{-3/2}{k} \frac{dx}{x^g} = (-1)^g \binom{-3/2}{g-1} = (-1)^g \binom{-1/2}{g} (-2g). \end{aligned}$$

The coordinates $L_j(0, \dots, 0)$ for $j > 2$ are calculated similarly. \square

Lemma 7.2. *We have*

$$(7.3) \quad L(\lambda) = \sum_{(k_3, \dots, k_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g-1}} L_{k_3, \dots, k_{2g+1}} \lambda_3^{k_3} \dots \lambda_{2g+1}^{k_{2g+1}},$$

where

$$(7.4) \quad L_{k_3, \dots, k_{2g+1}} = (-1)^g \binom{-1/2}{k_3 + \dots + k_{2g+1} + g} \prod_{i=3}^{2g+1} \binom{-1/2}{k_i} \\ \times (1, -2k_3 - \dots - 2k_{2g+1} - 2g, 2k_3 + 1, \dots, 2k_{2g+1} + 1).$$

Proof. The proof is similar to the proof of Lemma 7.1. \square

Using formula (4.5) we may reformulate (7.4) as

$$(7.5) \quad L_{k_3, \dots, k_{2g+1}} = 4^{-2(k_3 + \dots + k_{2g+1}) - g} \\ \times \binom{2(k_3 + \dots + k_{2g+1} + g)}{k_3 + \dots + k_{2g+1} + g} \binom{2k_3}{k_3} \cdots \binom{2k_{2g+1}}{k_{2g+1}} \\ \times (1, -2k_3 - \dots - 2k_{2g+1} - 2g, 2k_3 + 1, \dots, 2k_{2g+1} + 1).$$

7.4. Coefficients, nonzero modulo p . Given $(k_3, \dots, k_{2g+1}) \in \mathbb{Z}_{\geq 0}^{2g-1}$, let

$$k_i = k_i^0 + k_i^1 p + \dots + k_i^a p^a, \quad 0 \leq k_i^j \leq p-1, \quad i = 3, \dots, 2g+1,$$

be the p -ary expansions. Assume that a is such that not all numbers k_i^a , $i = 3, \dots, 2g+1$, are equal to zero. By Lemma 4.2, the product $\prod_{i=3}^{2g+1} \binom{2k_i}{k_i}$ is not congruent to zero modulo p if and only if

$$(7.6) \quad k_i^j \leq \frac{p-1}{2} \quad \text{for all } i, j.$$

Assume that condition (7.6) holds. Then for any $j = 0, \dots, a$, we have

$$\sum_{i=3}^{2g+1} k_i^j \leq (2g-1) \frac{p-1}{2} = gp - g - \frac{p-1}{2} < gp.$$

Define the *shift coefficients* (m_0, \dots, m_{a+1}) as follows. Namely, put $m_0 = g$. We have $\sum_{i=3}^{2g+1} k_i^0 + g < gp$. Hence there exists a unique integer m_1 , $0 \leq m_1 < g$, such that

$$0 \leq \sum_{i=3}^{2g+1} k_i^0 + g - m_1 p < p.$$

We have $\sum_{i=3}^{2g+1} k_i^1 + m_1 < gp$. Hence there exists a unique integer m_2 , $0 \leq m_2 < g$, such that

$$0 \leq \sum_{i=3}^{2g+1} k_i^1 + m_1 - m_2 p < p,$$

and so on. We have $0 \leq m_j < g$ for all $j = 1, \dots, a+1$.

We say that a tuple (k_3, \dots, k_{2g+1}) is *admissible* if it has property (7.6) and its shift coefficients (m_0, \dots, m_{a+1}) satisfy the system of inequalities

$$(7.7) \quad \sum_{i=3}^{2g+1} k_i^j - m_{j+1} p + m_j \leq \frac{p-1}{2}, \quad j = 0, \dots, a.$$

Theorem 7.3. *We have $L_{k_3, \dots, k_{2g+1}} \not\equiv 0 \pmod{p}$ if and only if the tuple (k_3, \dots, k_{2g+1}) is admissible. The tuple (k_3, \dots, k_{2g+1}) is admissible, if and only if $(k_3^j, \dots, k_{2g+1}^j) \in \Delta_{m_j}^{m_j+1}$ for $j = 0, \dots, a$, where the sets Δ_s^r are defined in (5.1). If the tuple (k_3, \dots, k_{2g+1}) is admissible, then modulo p we have*

$$(7.8) \quad L_{k_3, \dots, k_{2g+1}} \lambda_3^{k_3} \dots \lambda_{2g+1}^{k_{2g+1}} \equiv (-1)^{a(p-1)/2} \binom{2m_{a+1}}{m_{a+1}} \\ \times \left(\prod_{j=1}^a C_{m_j; k_3^j, \dots, k_{2g+1}^j}^{m_j+1} (\lambda_3^{p^j}, \dots, \lambda_{2g+1}^{p^j}) \right) K_{k_3^0, \dots, k_{2g+1}^0}^{m_1} (\lambda_3, \dots, \lambda_{2g+1}),$$

where $C_{s; \ell}^r(\lambda)$ are terms of the Cartier-Manin matrix expansion in (6.2) and $K_\ell^m(\lambda)$ are the terms of the expansion in (5.6) of the solution $J^m(z)$.

Proof. We have $L_{k_3, \dots, k_{2g+1}} \not\equiv 0 \pmod{p}$ if and only if each of the binomial coefficients in (7.5) is not divisible by p . For all $i = 3, \dots, 2g+1$, we have $\binom{2k_i}{k_i} \not\equiv 0 \pmod{p}$ if and only if property (7.6) holds.

The p -ary expansion of $k_3 + \dots + k_{2g+1} + g$ is

$$k_3 + \dots + k_{2g+1} + g = \left(\sum_{i=3}^{2g+1} k_i^0 - m_1 p + g \right) \\ + \left(\sum_{i=3}^{2g+1} k_i^1 - m_2 p + m_1 \right) p + \dots + \left(\sum_{i=3}^{2g+1} k_i^a - m_{a+1} p + m_a \right) p^a + m_{a+1} p^{a+1}.$$

By Lemma 4.2, the binomial coefficient $\binom{2(k_3 + \dots + k_{2g+1} + g)}{k_3 + \dots + k_{2g+1} + g}$ is not divisible by p if and only if inequalities (7.7) hold. Thus $L_{k_3, \dots, k_{2g+1}} \not\equiv 0 \pmod{p}$ if and only if the tuple (k_3, \dots, k_{2g+1}) is admissible.

The statement that the tuple (k_3, \dots, k_{2g+1}) is admissible, if and only if $(k_3^j, \dots, k_{2g+1}^j) \in \Delta_{m_j}^{m_j+1}$ for $j = 0, \dots, a$, follows from the definition of the sets Δ_s^r .

The last statement of the theorem is a straightforward corollary of Lucas's theorem, formulas for $C_{s; \ell}^r(\lambda)$, $K_\ell^m(\lambda)$, and the fact that $4^{kp} \equiv 4^k \pmod{p}$ for any k . \square

7.5. Decomposition of $L(\lambda)$ into the disjoint sum of polynomials. Define a set

$$(7.9) \quad M = \{(m_0, \dots, m_{a+1}) \mid a \in \mathbb{Z}_{\geq 0}, m_0 = g, m_j \in \mathbb{Z}_{\geq 0}, m_j < g \text{ for } j = 1, \dots, a+1\}.$$

For any $\vec{m} = (m_0, \dots, m_{a+1}) \in M$, define the $2g+1$ -vector of polynomial in $\lambda = (\lambda_3, \dots, \lambda_{2g+1})$:

$$(7.10) \quad K_{\vec{m}}(\lambda) = (-1)^{a(p-1)/2} \binom{2m_{a+1}}{m_{a+1}} \\ \times \left(\prod_{j=1}^a C_{m_j}^{m_j+1} (\lambda_3^{p^j}, \dots, \lambda_{2g+1}^{p^j}) \right) K^{m_1}(\lambda_3, \dots, \lambda_{2g+1}).$$

Notice that for $\vec{m}, \vec{m}' \in M$, $\vec{m} \neq \vec{m}'$, the set of monomials, entering with nonzero coefficients the polynomial $K_{\vec{m}}(\lambda)$, does not intersect the set of monomials, entering with nonzero coefficients the polynomial $K_{\vec{m}'}(\lambda)$.

Corollary 7.4. *We have*

$$(7.11) \quad L(\lambda) \equiv \sum_{\vec{m} \in M} K_{\vec{m}}(\lambda) \pmod{p}.$$

Notice that by Lemma 7.2, $L(\lambda)$ is a power series in λ with coefficients in $\mathbb{Z}^{2g+1}[\frac{1}{2}]$ independent of p , while the right-hand side in (7.11) is a formal infinite sum of polynomials in λ with coefficients in \mathbb{F}_p^{2g+1} and with nonintersecting supports.

7.6. Distinguished solution over \mathbb{C} and solutions $J^m(z)$ over \mathbb{F}_p . Let us compare the distinguished solution $I(z) = (z_2 - z_1)^{-1/2-g} L(\lambda(z))$ in (7.1), and the expansion (7.11). For any $\vec{m} = (m_0, \dots, m_{a+1}) \in M$, define

$$(7.12) \quad J_{\vec{m}}(z) = (z_2 - z_1)^{(p-1)/2-g+m_{a+1}p^{a+1}+(p+\dots+p^a)(p-1)/2} K_{\vec{m}} \left(\frac{z_3 - z_1}{z_2 - z_1}, \dots, \frac{z_{2g+1} - z_1}{z_2 - z_1} \right).$$

Theorem 7.5. *The following statements hold.*

- (i) *For any $\vec{m} \in M$, we have $J_{\vec{m}}(z) \in \mathbb{F}_p[z]^{2g+1}$.*
- (ii) *For any $\vec{m} \in M$, the polynomial vector $J_{\vec{m}}(z)$ is a solution of the KZ equations (2.2).*
- (iii) *The $\mathbb{F}_p[z^p]$ -module spanned by $J_{\vec{m}}(z)$, $\vec{m} \in M$, coincides with the $\mathbb{F}_p[z^p]$ -module $\mathcal{M}_{g,p}$ spanned by $I^m(z)$, $m = 0, \dots, g-1$.*

Proof. We have

$$\begin{aligned} J_{\vec{m}}(z) &= (-1)^{a(p-1)/2} \binom{2m_{a+1}}{m_{a+1}} \\ &\times \prod_{j=1}^a (z_2 - z_1)^{((p-1)/2-m_j+m_{j+1}p)p^j} C_{m_j}^{m_{j+1}} \left(\left(\frac{z_3 - z_1}{z_2 - z_1} \right)^{p^j}, \dots, \left(\frac{z_{2g+1} - z_1}{z_2 - z_1} \right)^{p^j} \right) \\ &\times (z_2 - z_1)^{(p-1)/2-g+m_1p} K^{m_1} \left(\frac{z_3 - z_1}{z_2 - z_1}, \dots, \frac{z_{2g+1} - z_1}{z_2 - z_1} \right), \end{aligned}$$

where

$$(z_2 - z_1)^{(p-1)/2-g+m_1p} K^{m_1} \left(\frac{z_3 - z_1}{z_2 - z_1}, \dots, \frac{z_{2g+1} - z_1}{z_2 - z_1} \right) = J^{m_1}(z)$$

is a solution of the KZ equations (2.2), see (5.6), and each factor

$$(z_2 - z_1)^{((p-1)/2-m_j+m_{j+1}p)p^j} C_{m_j}^{m_{j+1}} \left(\left(\frac{z_3 - z_1}{z_2 - z_1} \right)^{p^j}, \dots, \left(\frac{z_{2g+1} - z_1}{z_2 - z_1} \right)^{p^j} \right)$$

is a polynomial in $\mathbb{F}_p[z^p]$. This proves parts (i-ii) of the theorem. Part (iii) follows from the identity

$$K_{\vec{m}=(g,m_1)}(z) = \binom{2m_1}{m_1} J^{m_1}(z).$$

□

REFERENCES

- [AH] J. Achter, E. Howe, *Hasse-Witt and Cartier-Manin matrices: A warning and a request*, [arXiv:1710.10726](#), 1–14
- [Cl] H.C. Clemens, *A scrapbook of complex curve theory*, Second edition, Graduate Studies in Mathematics, **55**, AMS, Providence, RI, 2003. xii+188 pp
- [EFK] P. Etingof, I. Frenkel, A. Kirillov, *Lectures on representation theory and Knizhnik-Zamolodchikov equations*, Mathematical Surveys and Monographs, 58. AMS, Providence, RI, 1998. xiv+198 pp. ISBN: 0-8218-0496-0
- [KZ] V. Knizhnik and A. Zamolodchikov, *Current algebra and the Wess-Zumino model in two dimensions*, Nucl. Phys. **B247** (1984), 83–103
- [Ig] J. Igusa, *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Ac. Sci. USA, 44 (1958), 312–314
- [K] N. Katz, *Expansion-coefficients as approximate solutions of differential equations*, Asterisque **119-120** (1984), 183–189
- [L] E. Lucas, *Theorie des Fonctions Numeriques Simplement Priodiques*, American Journal of Mathematics. 1 (2) (1878) 184–196, doi:10.2307/2369308, JSTOR 2369308, MR 1505161
- [Ma] Y.I. Manin, *The Hasse-Witt matrix of an algebraic curve*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **25** (1961), 153–172
- [SV1] V. Schechtman and A. Varchenko, *Integral Representations of N-Point Conformal Correlators in the WZW Model*, Bonn, Max-Planck Institute, 1989, 1?22
- [SV2] V. Schechtman, A. Varchenko, *Arrangements of Hyperplanes and Lie Algebra Homology*, Invent. Math. **106** (1991), 139–194
- [SV3] V. Schechtman, A. Varchenko, *Solutions of KZ differential equations modulo p*, [arXiv:1707.02615](#), 1–23
- [V1] A. Varchenko, *The Euler beta-function, the Vandermonde determinant, the Legendre equation, and critical values of linear functions on a configuration of hyperplanes, I.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 53 (1989), no. **6**, 1206–1235, 1337; translation in Math. USSR-Izv. **35** (1990), no. 3, 543–571
- [V2] A. Varchenko, *Special functions, KZ type equations, and Representation theory*, CBMS, Regional Conference Series in Math., n. 98, AMS (2003)
- [V3] A. Varchenko, *Remarks on the Gaudin model modulo p*, [arXiv:1708.06264](#), 1–16
- [V4] A. Varchenko, *Solutions modulo p of Gauss-Manin differential equations for multidimensional hypergeometric integrals and associated Bethe ansatz*, [arXiv:1709.06189](#), Mathematics 2017, 5(4), 52; doi:10.3390/math5040052, 1–18