Modular-type functions attached to Calabi-Yau varieties: integrality properties

HOSSEIN MOVASATI and KHOSENO M. SHOKRI

Abstract

We study the integrality properties of the coefficients of the mirror map attached to the generalized hypergeometric function \( {}_nF_{n-1} \) with rational parameters and with a maximal unipotent monodromy. We present a conjecture on the \( p \)-integrality of the mirror map which can be verified experimentally. We prove its consequence on the \( N \)-integrality of the mirror map for the particular cases \( 1 \leq n \leq 4 \). We also give a straightforward and short proof of the only if part of the conjecture for arbitrary \( n \). This was a conjecture in mirror symmetry which was first proved in particular cases by Lian-Yau. The general format was formulated by Zudilin and finally established by Krattenthaler-Rivoal. For \( n = 2 \) we obtain the Takeuchi’s classification of arithmetic triangle groups with a cusp, and for \( n = 4 \) we prove that 14 examples of hypergeometric Calabi-Yau equations are the full classification of hypergeometric mirror maps with integral coefficients. For our purpose we state and prove a refinement of a theorem of Dwork which largely simplifies many existing proofs in the literature. As a by-product we get the integrality of the corresponding algebra of modular-type functions. These are natural generalizations of the algebra of classical modular and quasi-modular forms in the case \( n = 2 \).

1 Introduction

The integrality of the coefficients of the mirror map is a central problem in the arithmetic of Calabi-Yau varieties and it has been investigated in many recent articles [12, 18, 15, 10, 11]. The central tool in all these works has been the so called Dwork method developed in [5, 6]. It seems to us that the full consequences of Dwork method has not been explored, that is, to classify all hypergeometric differential equations with a maximal unipotent monodromy whose mirror maps have integral coefficients. In this article, we fill this gap and give a computable condition on the parameters of a hypergeometric function which conjecturally computes all the primes which appear in the denominators of the coefficients of the mirror map. We verify this conjecture and some of its consequences in many particular cases and give many computational evidence for its validness. Our short proofs of the integrality of mirror maps and Dwork’s theorem largely simplify the existing proofs in the literature and in particular [11].

Let \( a_i, \ i = 1, 2, \ldots, n \) be rational numbers, \( 0 < a_i < 1 \), \( a = (a_1, a_2, \ldots, a_n) \) and

\[
F(a|z) := {}_nF_{n-1}(a_1, \ldots, a_n; 1, 1, \ldots, 1|z) = \sum_{k=0}^{\infty} \frac{(a_1)_k \cdots (a_n)_k}{k!^n} z^k, \quad |z| < 1
\]

be the holomorphic solution of the generalized hypergeometric differential equation

\[
\theta^n - z(\theta + a_1)(\theta + a_2)\cdots(\theta + a_n) = 0
\]

where \( (a_i)_k = a_i(a_i+1)(a_i+2)\cdots(a_i+k-1) \), \( (a_i)_0 = 1 \), is the Pochhammer symbol and \( \theta = z \frac{d}{dz} \). The first logarithmic solution in the Frobenius basis around \( z = 0 \) has the form

\(1\)
\(G(a|z) + F(a|z) \log z\), where

\[
G(a|z) = \sum_{k=1}^{\infty} \frac{(a_1)_k \cdots (a_n)_k}{(k!)^n} \left[ \sum_{j=1}^{n} \sum_{i=0}^{k-1} \frac{1}{a_j + i} - \frac{1}{1 + i} \right] z^k.
\]

The mirror map

\[q(a|z) = z \exp\left( \frac{G(a|z)}{F(a|z)} \right),\]

is a natural generalization of the Schwarz function.

For a prime \(p\) and a formal power series \(f \in \mathbb{Q}[[z]]\) with rational coefficients we say that \(f\) is \(p\)-integral if \(p\) does not appear in the denominator of its coefficients or equivalently \(f\) induces a formal power series in \(\mathbb{Z}_p[[z]]\). For a rational number \(x\) such that \(p\) does not divide the denominator of \(x\), we define

\[\delta_p(x) := \frac{x + x_0}{p},\]

where \(0 \leq x_0 \leq p - 1\) is the unique integer such that \(p\) does not divide the denominator of \(\delta_p(x)\). We call \(\delta_p\) the Dwork operator. Throughout the text we call \(p\) a good prime if the denominators of \(a_i, \ i = 1, 2, \ldots, n\) are not divisible by \(p\) and call it a bad prime otherwise.

**Conjecture 1.** Let \(q(a|z)\) be the mirror map of the generalized hypergeometric function, defined as above, and let \(p\) be a good prime. Then \(q(a|z)\) is \(p\)-integral if and only if

\[
\{\delta_p(a_1), \delta_p(a_2)\} = \{a_1, a_2\}, \text{ or } \{1 - a_1, 1 - a_2\} \text{ for } n = 2
\]

and

\[
\{\delta_p(a_1), \delta_p(a_2), \delta_p(a_3), \ldots, \delta_p(a_n)\} = \{a_1, a_2, a_3, \ldots, a_n\}, \text{ for } n \neq 2.
\]

The conjecture for \(n = 1\) is an easy exercise. Due to the Euler identity for the Gauss hypergeometric function, the case \(n = 2\) appears different from other cases, see §3.1. For general \(n\) we prove the only if part and give computational evidence for the validity of the other direction, see §3.4. In the literature one is mainly interested to classify all \(N\)-integral mirror maps. This means that there is a natural number \(N\) such that \(q(a|Nz)\) has integral coefficients. The Conjecture 1 easily implies

**Conjecture 2.** The mirror map \(q(a|z)\) is \(N\)-integral if and only if for any good prime \(p\) we have (3) for \(n = 2\) and (4) for \(n \geq 3\).

**Theorem 1.** We have

1. For an arbitrary \(n\) the only if part of Conjecture 1 and Conjecture 2 are true.

2. Conjecture 2 for \(n = 1, 2, 3, 4\) is true.

The first part of the above theorem together with an exact formula for the smallest number \(N\) (see Theorem 2) was a conjecture in the context of mirror symmetry. The case \(a_i = \frac{i}{n+1}, \ i = 1, 2, \ldots, n\), where \(n+1\) is a prime number (resp. power of a prime number) is proved by Lian-Yau in [12] (resp. by Zudilin in [18]). In this generality, it is formulated by Zudilin in [18] and is proved by and Krattenthaler-Rivoal in [11]. Our approach using Dwork map \(\delta_p\) and a refinement of Dwork’s theorem simplifies largely the existing proofs in the literature. According to Conjecture 2 the \(N\)-integrality of the mirror map implies that for a fixed good prime \(p\) the map \(\delta_p\) acts
on the set \( \{a_1, \ldots, a_n\} \) as a permutation. This set is decomposed into subsets of cardinality \( \phi(m_i) \), \( m_i > 1 \), \( i = 1, 2, \ldots, k \), where \( \phi \) is the arithmetic Euler function. This is done according to whether two elements have the same denominator or not. The numbers \( m_i, \ i = 1, 2, \ldots \) are all possible denominators in the set \( \{a_1, \ldots, a_n\} \). Such a decomposition is invariant under the permutation induced by \( \delta_p \). We conclude that the number of \( N \)-integral mirror maps is equal to the number of decompositions:

\[
\delta(n) = \phi(m_1) + \cdots + \phi(m_k)
\]

Like in the classical case of the partition of a number with natural numbers we have the following generating function:

\[
24x^2 - 1 + \prod_{m=2}^{\infty} \frac{1}{1 - x^{\phi(m)}} = x + 28x^2 + 4x^3 + 14x^4 + 14x^5 + 40x^6 + 40x^7 + \cdots.
\]

(for the coefficient of \( x^2 \) see Table 1). Conjecture 2 says that the coefficient of \( x^n \) counts the number of \( N \)-integral mirror maps with \( n \)-parameters \( a_1, a_2, \ldots, a_n \). An immediate consequence of (5) is that the number of \( N \)-integral mirror maps for \( n = 2\ell + 1, \ \ell \geq 2 \) exactly equals with \( n = 2\ell \) ones. Since \( \phi(m) \), for \( m > 2 \) is even, for \( n = 2\ell + 1 \) in the right hand side of (5), one of the \( m_i \)'s is 2 or equivalently one of \( a_i \) is \( \frac{1}{2} \). After canceling this from both sides we return to the case \( n = 2\ell \). Therefore, the number of \( N \)-integral mirror maps for \( n = 2\ell \) and \( 2\ell + 1 \) are in a one to one correspondence.

For any fixed \( n \), we can use conjecture 2 and classify all \( N \)-integral mirror maps. For instance for \( n = 2 \), the mirror map is \( N \)-integral if and only if \( \{a_1, a_2\} \) belongs to the list in Table 1. The first four cases correspond to \( \{\delta_p(a_1), \delta_p(a_2)\} = \{a_1, a_2\} \) and the others correspond to \( \{\delta_p(a_1), \delta_p(a_2)\} = \{1 - a_1, 1 - a_2\} \). If we set \( \{a_1, a_2\} = \left\{ \frac{1}{2} \left( 1 \pm \frac{1}{m_1} - \frac{1}{m_2} \right) \right\} \) with \( m_1, m_2 \in \mathbb{N} \) and \( \frac{1}{m_1} + \frac{1}{m_2} > 1 \) then the monodromy group of the Gauss hypergeometric equation (1) is a triangle group of type \( (m_1, m_2, \infty) \). In this case the above classification is reduced to the Takeuchi's classification in [17] of arithmetic triangle groups with a cusp, see [3].

For \( n \geq 4 \) even and with an \( N \)-integral mirror map \( q(a|z) \), the set \( \{a_1, a_2, \ldots, a_n\} \) is conjecturally invariant under \( x \mapsto 1 - x \), see §2.1 and so we may identify \( a = (a_1, a_2, \ldots, a_n) \) with its \( \frac{n}{2} \) elements in the interval \([0, \frac{1}{2}]\). Below we just list these elements. The case \( n = 4 \) has many applications in mirror symmetry. We find that \( q(a|z) \) is \( N \)-integral if and only if \( (a_1, a_2, a_3, a_4) \) belongs to the well-known 14 hypergeometric cases of Calabi-Yau equations. The first two elements \( (a_1, a_2) \) are given in Table 1. Note that in [4], these 14 cases are classified through properties of the monodromy group of the differential equation (1) which comes from the variation of Hodge structures of Calabi-Yau varieties. The fact that the corresponding mirror maps are \( N \)-integral and are the only ones with this property is a non-trivial statement. For \( n = 6 \) we find 40 examples of \( N \)-integral mirror maps. In this case \( (a_1, a_2, a_3) \) are given in Table 1. Finding 40 examples of one parameter families of Calabi-Yau varieties of dimension 5 may be done in a similar way as in the \( n = 4 \) case. This is left for a future work. Note that for an arbitrary \( n \) the Picard-Fuchs equation of the Dwork family \( x_1^{n+1} + \cdots + x_{n+1}^{n+1} - (n + 1)z^{-\frac{1}{n+1}}x_1x_2 \cdots x_{n+1} = 0 \) corresponds to the case \( a_i = \frac{i}{n+1}, \ i = 1, 2, \ldots, n \).

The discussion for \( n = 2 \) suggests that the \( N \)-integrality of the mirror map is related to the arithmeticity of the monodromy group of (1). However, note that for \( n = 4 \) it is proved that the seven of the fourteen examples are thin, that is, they have infinite index in \( \text{Sp}(4, \mathbb{Z}) \), see [2]. Note also that, we know a complete classification of the Zariski closure of the monodromy group of (1), see [1]. Since in [13] we have constructed a new kind of modular forms theory for these examples of thin groups, see also §3.5, it is reasonable to weaken the notion of arithmeticity so
that the monodromy group of (1) with an \(N\)-integral mirror map becomes arithmetic in this new sense. For a discussion of thin groups and their applications see Sarnak's lecture notes [16] and the references therein.

Finding the smallest \(N\) is not a trivial problem and is discussed in the articles [12, 18, 11] for particular cases. Along the way to prove Theorem 1 we also prove

**Theorem 2.** Let \(a_1, a_2, \ldots, a_{r_p}\) be all parameters \(a_i\) whose denominator is divisible by \(p\). Set

\[
N_p := p^{r_p}, \quad c_p := \sum_{i=1}^{r_p} \text{ord}_p \text{denominator} (a_i) + \left\lceil \frac{r_p}{p-1} \right\rceil
\]

Let us define \(\delta_p(a_i) := a_i, \quad i = 1, 2, \ldots, r_p\) and assume (3) for \(n = 2\) and (4) for \(n \geq 3\). Then the mirror map \(q(N_p z)\) is \(p\)-integral.

Note that if \(p\) is a good prime, that is \(r_p = 0\), then \(c_p = 0\). Using this theorem we know that for an \(N\)-integral mirror map

\[
N := \prod_p N_p,
\]

is the smallest \(N\) such that \(q(N z) \in \mathbb{Z}[[z]]\).

**Corollary 1.** Let \(n = 4\) and consider one of the fourteen cases in Table 1. Let also \(z(q)\) be the inverse of the mirror map \(q(z) := q(a z)\) and

\[
u_0 := z, \quad u_i := \theta^i F, \quad i = 0, 1, 2, 3, \quad u_{i+4} := F\theta^i G - G\theta^i F, \quad i = 1, 2.
\]

We have

\[
\frac{1}{N} u_0(q), u_i(z(q)) \in \mathbb{Z}[[q]], \quad i = 0, 1, \ldots, 6.
\]

The field of modular-type functions is generated by (8) and it is invariant under \(q \frac{\partial}{\partial q}\). There are many analogies between \(\mathbb{Q}(u_i(z(q)), \quad i = 0, 1, \ldots, 6)\) and the field of quasi-modular forms, see for instance [13]. This includes functional equations with respect to the monodromy group of (1), the corresponding Halphen equation and so on. However, note that the former field is of transcendental degree 3, whereas this new field is of transcendental degree 7. For \(n = 2\) a similar discussion as in Corolary 1 leads us to the theory of (quasi) modular forms for the monodromy group of (1), see for instance [3].

We would like to thank M. Belolipetsky for taking our attention to the works on thin groups. Thanks also go to P. Sarnak, S. T. Yau, F. Beukers and W. Zudilin for comments on the first draft of the present text. The second author would like to thank CNPq-Brazil for financial support and IMPA for its lovely research ambient.

In the the final steps of the present text, F. Beukers informed us about the article [14] in which the author proves Conjecture 3 in §3 using results in differential Galois theory. As a consequence the if part of the Conjecture 2 follows easily. Our proof of the Conjecture 2 for \(n = 1, 2, 3, 4\) is elementary and self-content. Note also that the main contributions of the present text are a refinement and a short proof of Dwork’s theorem and a short proof of the integrality conjecture proved in [11].
2 Dwork’s theorem

As far as we know, the main argument in the literature for proving the \( p \)- or \( N \)-integrality of mirror maps is the work of B. Dwork in \([6, 5]\). However, it seems to us that Dwork’s work is not fully employed or understood. This lies maybe in the heavy \( p \)-adic machinery of Dwork’s work which makes his articles difficult to read. In this section, we give a refinement of a theorem of Dwork and prove it. The reformulation of these results for other linear differential equations, and in particular Calabi-Yau equations in the sense of \([8]\), is a work for future, see for instance \([15]\).

2.1 Dwork map

The Dwork map is defined in the following way

\[
\delta_p : \mathbb{Z}_p \to \mathbb{Z}_p, \quad \sum_{s=0}^{\infty} x_s p^s \mapsto 1 + \sum_{s=0}^{\infty} x_{s+1} p^s, \quad 0 \leq x_s \leq p - 1 \tag{9}
\]

(and so \( p\delta_p(x) - x = p - x_0 \) for \( x \in \mathbb{Z}_p \)). Let \( \mathbb{Z}_p \) be the set of \( p \)-integral rational numbers. We have a natural embedding \( \mathbb{Z}_p \to \mathbb{Z}_p \). The map \( \delta_p \) leaves \( \mathbb{Z}_p \) invariant because for \( x \in \mathbb{Z}_p \), \( \delta_p(x) \) is the unique number such that \( p\delta_p(x) - x \in \mathbb{Z}_p \setminus \{0, p - 1\} \). For a rational number \( x = \frac{a}{x_2}, \ x_1, x_2 \in \mathbb{Z} \) and a prime \( p \) which does not divide \( x_2 \), we have

\[
\delta_p(x) := \frac{p^{-1} x_1 \mod x_2}{x_2},
\]

where \( p^{-1} \) is the inverse of \( p \) mod \( x_2 \) and \( x_1 \) and \( x_2 \) may have common factors. The denominators of \( x \) and \( \delta_p(x) \) are the same and \( \delta_p(1-x) = 1 - \delta_p(x) \). For any finite set of rational numbers, there is a finite decomposition of prime numbers such that in each class the function \( \delta_p \) is independent of the prime \( p \).

The following proposition easily follows from (9). It will play an important role in the proof of Theorem 1.

**Proposition 1.** Let \( 0 < x = \frac{x_1}{sq^y} < 1 \) be a rational number, where \( q \) is a prime and \((q, s) = 1 \) and \( t \) and \( sq^y \) may have common factors. We have

1. For primes \( p \) such that \( p^{-1} \equiv -1 \pmod{sq^y} \) we have \( \delta_p(x) = 1 - x \).

2. If \( y = 0 \), that is the denominator of \( x \) is not divisible by \( q \), then for primes \( p \) such \( p^{-1} \equiv q \pmod{s} \) we have

\[
\delta_p(x) = qx - i, \quad \text{for some } i = 0, 1, 2, \ldots, q - 1.
\]
3. For primes $p^{-1} \equiv s + q \pmod{sq^y}$ we have

$$\delta_p(x) = qx + \frac{r}{q^y} - i, \text{ for some } r = 0, 1, \ldots, q^y - 1, i = 0, 1, \ldots, q$$

4. If $y \geq 1$, that is, the denominator of $x$ may be divisible by $q$, then for any $0 \leq m \leq y$ and prime $p$ with $p^{-1} \equiv 1 + q^y - m s \pmod{sq^y}$ either we have $\delta_p(x) = x$ or we have

$$\delta_p(x) = x + \frac{r}{q^m} - i, \text{ for some } r = 1, \ldots, q^m - 1, i = 0, 1.$$

### 2.2 Dwork lemma and theorem on hypergeometric functions

In this section we mention some lemmas and a refinement of a theorem of Dwork. The following lemma is crucial in the argument of $N$-integrality of the mirror map. Since the non trivial application of this lemma was first given by Dwork, it is known as Dwork lemma, however, Dwork himself in [7] associates it to Dieudonné.

**Lemma 1.** Let $f(z) \in 1 + z\mathbb{Q}_p[[z]]$. Then $f(z) \in 1 + z\mathbb{Z}_p[[z]]$, if and only if $f(z^p) = (f(z))^p \in 1 + p\mathbb{Z}_p[[z]]$.

For a more general statement and the proof see [7], p.54.

**Lemma 2.** Let $x$ be a rational number and $p$ be prime which does not divide the denominator of $x$. We have

$$(x)_{\ell p} = (x)_{\ell p} \equiv (\delta_p(x))_{\ell} \pmod{p\mathbb{Z}_p}, \forall \ell \in \mathbb{N}.$$

**Proof.** For $0 \leq j \leq \ell - 1$, the set $\{x + i + jp|0 \leq i \leq p - 1\}$ is a complete set of residue modulo $p$. Now assume that for some $0 \leq i_0 < p, p|(x + i_0)$, so by definition we have $x + i_0 = p\delta_p(x)$. The terms divisible by $p$ has the form $x + i_0 + jp$. Hence we have

$$\frac{(x)_{\ell p}}{(\ell p)!} \equiv \frac{\prod_{j=0}^{\ell-1}(x + i_0 + jp)}{\prod_{j=1}^{\ell} j p} \pmod{p\mathbb{Z}_p}$$

$$\equiv \frac{\prod_{j=0}^{\ell-1}((\delta_p(x) + j)p)}{\prod_{j=1}^{\ell} j p} \pmod{p\mathbb{Z}_p}$$

$$\equiv \frac{(\delta_p(x))_{\ell}}{\ell!} \pmod{p\mathbb{Z}_p}.$$ 

**Lemma 3.** For any good prime $p$, we have $F(a|z) \in \mathbb{Z}_p[[z]]$.

**Proof.** For $x \in \mathbb{Q}$ and $k = k_0 + k_1 p + k_2 p^2 + \cdots + k_s p^s \in \mathbb{N}$ with $0 \leq k_i \leq p - 1$, we use Lemma 2 and we have

$$\frac{(x)_{k}}{k!} \equiv \frac{(x)_{k_0}}{k_0!} \frac{(\delta_p x)_{k_1}}{k_1!} \cdots \frac{(\delta_p^{s-1} x)_{k_s}}{k_s!} \pmod{p\mathbb{Z}_p}.$$
Note that for \( k = k_0 + \ell p, \ 0 \leq k_0 < p \) we can separate \( \frac{(x)^k}{k!} \) in two pieces, namely

\[
\frac{(x)_{\ell p+k_0}}{\ell p+k_0)!} = \frac{(x)_{\ell p}}{\ell p)!} \cdot \frac{(x+\ell p)_{k_0}}{(\ell p+1)_{k_0}} \tag{11}
\]

Since \( 0 \leq k_0 < p \), we have

\[
\frac{(x+\ell p)_{k_0}}{(\ell p+1)_{k_0}} = \frac{(x)_{k_0}}{k_0)!} \equiv (x)_{k_0} \pmod{pZ_p}. \tag{12}
\]

For an integer \( k = k_0 + k_1 p + \cdots + k_s p^s \) we have

\[
\text{ord}_p(k!) = \frac{k - \sigma_k}{p - 1}, \quad \text{where} \quad \sigma_k = k_0 + k_1 + \cdots + k_s. \tag{13}
\]

In particular, for any \( r \in \mathbb{N} \)

\[
\text{ord}_p((k!)^r) \leq \frac{kr}{p - 1}. \tag{14}
\]

Note that for \( k = k_0 + \ell p, \ 0 \leq k_0 < p \) we have \( \text{ord}_p k! = \ell + \text{ord}_p \ell! \). Let \( c_p \) be the number \( 6 \) and define \( \delta_p(x) = x \) if \( p \) divides the denominator of \( x \). For a vector \( a = (a_1, \ldots, a_n) \) define \( \delta_p(a) := (\delta_p(a_1), \ldots, \delta_p(a_n)) \).

**Theorem 3.** Let \( a_i \)'s be rational numbers and let \( F \) and \( G \) be as in the Introduction. Let also \( p \) be any prime number. We have

1. \( Q(z) F(\delta_p(a)|N_p z^p) \equiv F(a|N_p z) \pmod{pZ_p[[z]]} \)
2. \( Q(z) G(\delta_p(a)|N_p z^p) \equiv pG(a|N_p z) \pmod{pZ_p[[z]]} \)

where \( Q(z) := F(a|N_p z) \pmod{z^p} \), is a polynomial of degree \( p - 1 \).

The above theorem is the core of Dwork’s theorem. We believe that in this new format (which includes bad primes and is written in two pieces) it simplifies many arguments in Dwork’s original work and the literature on the integrality of mirror maps. Indeed, in [5] Dwork represents the statement 1 for good primes as a congruency between coefficients and then directly concludes Theorem 4 without mentioning statement 2.

**Proof.** We first prove the theorem for good primes, that is, \( r_p = 0 \) and so \( c_p = 0 \). Below all congruences are \( \text{mod} \ pZ_p \). For the first congruence, it is enough to show it for \( n = 1 \). For general \( n \) it follows from \( n = 1 \) case. For \( k = k_0 + \ell p, \) with \( 0 \leq k_0 < p, \) the \( k \)th coefficient of the right hand side is simply \( \frac{(a_1)^k}{k!} \). The corresponding coefficient in the left hand side is \( \frac{(a_1)_{k_0} (\delta_p(a_1))_{\ell} }{k_0)! \ell!} \). The equality follows from (11), (12) and (10). Let

\[
H_x(k) := \sum_{i=0}^{k-1} \frac{1}{x+i}, \quad x \in \mathbb{Q}, \quad k \in \mathbb{N}
\]

be the harmonic sum. For the second part again without loss of generality we can assume that \( n = 1 \). This is because the \( k \)-th coefficient in the right hand side of item 2 in the theorem is the sum of \( n \)-terms

\[
\frac{(a_1)_{k} (a_2)_{k} \cdots (a_n)_{k}}{k! n} (H_{a_j}(k) - H_1(k)), \quad j = 1, 2, \ldots
\]
and by the first part with parameters $a_1, a_2, \ldots, a_n$ we have

$$\frac{(a_1)_k \cdot \cdots (a_j)_k \cdot \cdots (a_n)_k}{k!^{n-1}} = \frac{(a_1)_{k_0} \cdots (a_j)_{k_0} \cdots (a_n)_{k_0}}{k_0!^{n-1}} \frac{\delta_p a_1 \ell \cdots \delta_p a_j \ell \cdots \delta_p a_n \ell}{\ell!^{n-1}}.$$  

Note that by Lemma 3 both sides of this congruence are in $\mathbb{Z}_p$. For $n = 1$, again let $k = k_0 + \ell p$ as before. The $k$th coefficient of $G(a|z)$ can be written as a sum $S_1 + S_2$, where

$$S_1 = \frac{(a_1 + \ell p)_{k_0} (a_1)_{\ell p}}{(\ell p + 1)_{k_0} (\ell p)!} (H_a_{1,\ell p} - H_1(\ell p))$$

$$S_2 = \frac{(a_1 + \ell p)_{k_0} (a_1)_{\ell p}}{(\ell p + 1)_{k_0} (\ell p)!} (H_{a_1 + \ell p(k_0)} - H_{1 + \ell p(k_0)})$$

The term $S_2$ is $p$-integral and so $pS_2 \equiv 0 \pmod{p\mathbb{Z}_p}$. The term $p \cdot S_1$ is congruent to the desired term.

Now, let us consider a bad prime $p$. For simplicity we write $r = r_p$ and $c = c_p$. Let us first assume that $(p - 1)|r$. Let also $f(k) := \frac{k!}{k^{r_p - \sum k}}$ be the free of $p$ part of $k!$, where $\sigma_k$ is defined in (13). For $m = k_0 + p\ell$, $0 \leq k_0 < p$ we have

$$f(k) \equiv f(k_0)f(\ell)(-1)^\ell \pmod{p\mathbb{Z}_p}$$

This can be seen by writing

$$f(k) = f(\ell p)(\ell p)_{k_0 - 1} \equiv f(\ell)((p - 1)!)^{\ell}k_0! \pmod{p\mathbb{Z}_p}$$

Let $m_i$ be the order of the denominator of $a_i$ at $p$ and $b_i = p^{m_i}a_i$. The $k$-th coefficient of $F(a|N_p z)$ is

$$A_k := p^{-r_p \sum k} \prod_{i=1}^{r} \frac{\ell p^{m_i}}{(k!)^r} \prod_{i=r+1}^{n} \frac{(a_i)_k}{k!}$$

$$= p^{-r_p \sum k} \prod_{i=1}^{r} \frac{b_i^k}{f(k)^r} \prod_{i=r+1}^{n} \frac{(a_i)_{k_0} (a_i)_{\ell}}{k_0! \ell!}$$

$$= \frac{p^{-r_p \sum k}}{f(k_0)^r f(\ell)^r (-1)^\ell} \prod_{i=r+1}^{n} \frac{(a_i)_{k_0} (a_i)_{\ell}}{k_0! \ell!}$$

$$= A_{k_0} A_\ell$$

(15)

Note that if $p = 2$ then $(-1)^r = 1$ and if $p \neq 2$ then by our hypothesis $p - 1|r$ and so $r$ is even. This proves the first assertion for a bad prime $p$.

The $k$-th coefficient $pB_k$ of $pG(a|N_p z)$ is a sum of $n$-terms

$$pB_{k,j} := N^p_{k} \frac{(a_1)_k (a_2)_k \cdots (a_n)_k}{k!^{n}} (pH_{a_j}(k) - pH_1(k)), \quad j = 1, 2, \ldots, n$$

For $j = 1, 2, \ldots, r$ we have $H_{a_j}(k) \equiv 0$, $H_{a_j}(k_0) \equiv 0$ and $pH_1(k) \equiv H_1(\ell)$ and $pH_1(0) \equiv 0$. Therefore, $pB_{k,j} \equiv B_{\ell,j} A_{k_0}$. For $j = r + 1, \ldots, n$ the proof is as in the case $p$ a good prime.

If $(p - 1) \not| r$ then $r \neq 0$ and so $p$ appears in the denominator of at least one $a_i$. Therefore, by (15) $F \equiv 1$. In this case the first congruence is reduced to $1 \equiv 1$. In a similar way the second
congruence is an equality for all good primes \( p \). Furthermore if \( q \),

\[
\text{exp}(k) = \sum_{n=0}^\infty \frac{k^n}{n!} \]

Let \( \text{ord}_q B_k = \frac{\sigma_k}{p-1} - \lfloor \log_p k \rfloor \)

By Lemma 3 we have

**Proof.** Let \( F \) as before. We have

\[
\frac{G(a|N_p z^p)}{F(a|N_p z^p)} \equiv p \frac{G(a|N_p z)}{F(a|N_p z)} \pmod{p \mathbb{Z}_p[[z]]}.
\]

**Proof.** By Lemma 3 we have \( F_0 \in 1 + z \mathbb{Z}_p[[z]] \) and so \( \frac{1}{F_0} \) is also in the same ring. Hence statement 1 holds by replacing \( F_0 \) with \( \frac{1}{F_0} \). Now multiplying this new congruency with both sides of the congruency of statement 2 we get the result.

### 2.3 Consequences of Dwork’s theorem

The mirror map is the invertible function \( q(a|z) = z \exp \left( \frac{G(a|z)}{F(a|z)} \right) \). The inverse of the mirror map is important for the construction of modular-type functions. In this section we give conditions for integrality of the mirror map.

**Lemma 4.** Let \( a_1, a_2, \ldots, a_n \in \mathbb{Q} \) with the conditions (3) and (4) for a prime \( p \). Then

\[
q(a|N_p z) \in z \mathbb{Z}_p[[z]],
\]

**Proof.** Let \( f(z) = \frac{G(a|N_p z)}{F(a|N_p z)} \). Since \( f(z) \in z \mathbb{Q}[[z]] \), so \( \exp(f(z)) \in 1 + z \mathbb{Q}[[z]] \). Our assumption and Theorem 4 imply that

\[
f(z^p) - p f(z) = p \cdot g(z), \quad g(z) \in z \mathbb{Z}_p[[z]].
\]

Since \( \exp(p \cdot g(z)) = 1 + \sum_{k=1}^\infty \frac{p^k}{k!} g(z)^k \) and \( \text{ord}_p(k!) < k \), we find that

\[
\frac{\exp f(z^p)}{(\exp f(z))^p} = \exp(p \cdot g(z)) \in 1 + p z \mathbb{Z}_p[[z]].
\]

Now by applying Lemma 1, the result follows.

**Lemma 5.** If \( q(a|N_p z) \) is \( p \)-integral then

\[
(16) \quad \frac{G(\delta_p(a)|N_p z)}{F(\delta_p(a)|N_p z)} \equiv \frac{G(a|N_p z)}{F(a|N_p z)} \pmod{p \mathbb{Z}_p[[z]]}.
\]

Furthermore if \( q(z|N_p z) \) is \( p \)-integral for all except a finite number of primes then the above congruence is an equality for all good primes \( p \).
We conjecture that in Lemma 5, the congruence (16) is an equality. This together with Conjecture 3 in §3 imply Conjecture 1.

Proof. Let

\[ f(z) := \frac{G(a|N_p z)}{F(a|N_p z)}, \quad f'(z) := \frac{G(\delta_p(a)|N_p z)}{F(\delta_p(a)|N_p z)}. \]

By Lemma 1 exp(f) is p-integral if and only if \( \exp(f(z^p) - pf(z)) \in 1 + p\mathbb{Z}_p[[z]] \) and by Theorem 4 \( f'(z^p) \equiv pf(z) \pmod{p\mathbb{Z}_p[[z]]} \). Combining these two facts

\[ \exp(f(z^p) - f'(z^p)) \in 1 + p\mathbb{Z}_p[[z]]. \]

or \( f(z^p) - f'(z^p) = \log(1 + p z g(z)) \), for some \( g(z) \in \mathbb{Z}_p[[z]] \). But

\[ \log(1 + p z g(z)) = \sum_{n=1}^{\infty} (-1)^n \frac{p^n z^n g(z)^n}{n} \in p z\mathbb{Z}_p[[z]] \]

Now, let us prove the second part. Since the number of bad primes is finite, our hypothesis implies that \( q(a|z) \) is p-integral for all good primes except a finite number which may includes bad primes. Let \( c \) is the common factor of the denominators of \( a_i \)'s and let \( r \) be a prime residue of \( c \). From (9) for \( p \equiv r \pmod{c} \) the the value of \( \delta_p(a_i) \) is independent of the special member of this class of primes. On the other hand by assumption congruency (16) holds for almost all primes of this class and so it must be equality. Now running over all prime residues \( r \) gives the result. \[ \square \]

Remark 1. If the congruence (16) does not happen then by Lemma 5, \( q(a|N_p z) \) is not p-integral. In fact this turns out to be a fast way to check the non-p-integrality than checking the non p-integrality of \( q(a|N_p z) \) directly. For instance, for \( n = 2, p = 101, a_1 = 169/330, \quad a_2 = 139/330 \) the truncated \( q(a|z) \mod z^k, \quad k < 101 \) is p-integral but \( q(a|z) \) is not p-integral because the congruency (16) fails at the power \( z^2 \).

Lemma 6. If the mirror map \( q(a|z) \) is p-integral then \( q(\delta_p(a)|z) \) is also p-integral.

Proof. The proof follows directly from the congruency (16). Note that, if \( f \in p\mathbb{Z}_p[[z]] \), then \( e^f \in \mathbb{Z}_p[[z]] \). \[ \square \]

2.4 Proof of Theorem 1, part 1 and Theorem 2

The only if part of both conjectures 1 and 2 follows from Lemma 4. So, it remains to prove Conjecture 2 for \( n = 1, 2, 3, 4 \).

3 A problem in computational commutative algebra

The only missing step for the proof of Conjecture 2 is a solution to the following conjecture:

Conjecture 3. Let \( n \neq 2 \) and \( a_i, b_i \in \mathbb{Q}, \quad i = 1, 2, \ldots, n \) with \( 0 < a_i, b_i < 1 \), we have the equality of formal power series

\[ G(b_1, b_2, \ldots, b_n|z) = G(a_1, a_2, \ldots, a_n|z) \]

if and only if

\[ \{b_1, b_2, \ldots, b_n\} = \{a_1, a_2, \ldots, a_n\}. \]
Let
\[
\frac{G(a|z)}{F(a|z)} = \sum_{i=1}^{\infty} C_k(a)z^k, \quad C_k(a) \in \mathbb{Q}[a].
\]
and \(I_{n,m}\) be the ideal in \(\mathbb{Q}[a, b]\) generated by \(C_k(a) - C_k(b), \ k = 1, 2, \ldots, m\) and \(I_n = I_{n,\infty}\). The above conjecture over \(\mathbb{C}\) is false, that is, the variety given by \(I_n\) has many components other than those obtained by the permutation (18). Therefore, the above conjecture is equivalent to say that such extra components have no non-trivial \(\mathbb{Q}\)-rational points. We are planning to write a separate article on this topic. In this section we will try to avoid Conjecture 3 in such a general context. Instead, we will use the structure of the operator \(\delta_p\) in order to reduce the number of variables and try to solve Conjecture 3 for such particular cases. Below, we are going to write down the primary decomposition of \(I_{n,m}\) in the ring \(\mathbb{Q}[a, b]\) for many particular cases. We have used the Gianni-Trager-Zacharias algorithm implemented in 
\textbf{Singular} under the command \texttt{primdecGTZ}, see [9]. The corresponding computer codes can be found in the first author’s web page.

### 3.1 The case \(n = 2\)

The case \(n = 2\) is different because of the Euler identity. We have the primary decomposition

\[
I_{2,2} = \langle a_2 - b_2, a_1 - b_1 \rangle \cap \langle a_2 - b_1, a_1 - b_2 \rangle \cap \langle a_2 + b_2 - 1, a_1 + b_1 - 1 \rangle \cap \langle a_2 + b_1 - 1, a_1 + b_2 - 1 \rangle
\]
in the ring \(\mathbb{Q}[a, b]\). Therefore, the equality (3) is valid if and only if

\[
\{b_1, b_2\} = \{a_1, a_2\} \text{ or } \{1 - a_1, 1 - a_2\}.
\]

The second possibility for \(\{b_1, b_2\}\) is due to the Euler identity for the Gauss hypergeometric function \(2F_1(a, b, c|z) = \sum_{k=0}^{\infty} \frac{(a)_k(b)_k}{(k)_k(c)_k} z^k:\)

\[
2F_1(a, b, c|z) = (1 - z)^{c-a-b} 2F_1(c - a, c - b, c|z)
\]

Note that we put \(c = 1\) and the same equality is valid for the logarithmic solution. This proves Theorem 2 part 2 for \(n = 2\).

### 3.2 The symmetry

Let \(b_i = 1 - a_i, \ i = 1, 2, \ldots, n\) and let us restrict the ideal \(I_{n,m}\) to this locus. For \(n = 3\) we have the primary decomposition

\[
I_{3,3} = \langle a_2 + a_3 - 1, 2a_1 - 1 \rangle \cap \langle a_3 - 1, a_1 + a_2 - 1 \rangle \cap \langle 2a_2 - 1, a_1 + a_3 - 1 \rangle \cap \langle a_3 - 1, a_2 - 1, a_1 - 1 \rangle \cap \langle a_3, a_2, a_1 \rangle
\]

and for \(n = 4\) we have the primary decomposition

\[
I_{4,4} = \langle a_2 + a_3 - 1, a_1 + a_4 - 1 \rangle \cap \langle a_3 + a_4 - 1, a_1 + a_2 - 1 \rangle \cap \langle a_2 + a_4 - 1, a_1 + a_3 - 1 \rangle \cap \langle a_2 + a_3 - 2, a_1 + a_4 - 2 \rangle \cap \langle a_3 + a_4, a_2 + a_3 + a_1 + a_4 \rangle \cap \langle a_3 + a_4, a_2^2 + a_4, a_1 + a_2 \rangle \cap \langle a_3 + a_4, a_2^2 + a_3 + a_1 + a_4 \rangle \cap \langle a_3 + a_4, a_2^2 + a_3 + a_1 + a_4 \rangle \cap \langle a_3 + a_4, a_2 + a_4, a_1 + a_3 \rangle \cap \langle a_3 + a_4, a_2 + a_4 + 2, a_1 + a_3 - 2 \rangle \cap \langle a_3 + a_4, a_2 + a_4 + 2, a_1 + a_3 - 2 \rangle \cap \langle a_3 + a_4, a_2 + a_4 - 2, a_1 + a_3 - 2 \rangle \cap \langle a_3 + a_4, a_2^2 + a_3 + a_1 + a_4 \rangle \cap \langle a_3 + a_4, a_2 + a_4 + 2, a_1 + a_3 - 2 \rangle \cap \langle a_3 + a_4, a_2 + a_4 + 2, a_1 + a_3 - 2 \rangle \cap \langle a_3 + a_4, a_2 + a_4 - 2, a_1 + a_3 - 2 \rangle \cap \langle a_3 + a_4, a_2 + a_4, a_1 + a_3 \rangle \cap \langle a_3 + a_4, a_2 + a_4 + 2, a_1 + a_3 - 2 \rangle \cap \langle a_3 + a_4, a_2 + a_4 + 2, a_1 + a_3 - 2 \rangle \cap \langle a_3 + a_4, a_2 + a_4, a_1 + a_3 \rangle \cap \langle a_3 + a_4, a_2 + a_4 + 2, a_1 + a_3 - 2 \rangle.
\]

We conclude that Conjecture 3 is true for \(n = 3, 4\) and \(b_i = 1 - a_i\). Note that for \(n = 4\) the components which are not in the variety \(\{a_i, \ i = 1, 2, 3, 4\} = \{1 - a_i, \ i = 1, 2, 3, 4\}\) do not have \(\mathbb{Q}\)-rational points.
3.3 Proof of Theorem 1, part 2

The only missing step is the verification of Conjecture 3. The case $n = 1$ can be done by hand and the case $n = 2$ is done in §3.1. For $n \geq 3$ we do not get the primary decomposition of $I_{n,n}$ in Singular, therefore, we do not have a proof for Conjecture 3 with arbitrary parameters $a_i$ and $b_i$. However, we may try to prove it for particular classes of parameters $a_i, b_i$. The particular cases that appear in this section are motivated by the structure of $\delta_p$ described in Proposition 1.

First, let us take primes $p$ such that $\delta_p(x) = 1 - x$, see Proposition 1 item 1. In this case we have the primary decompositions in §3.2 which implies that the set of $a_i$'s is invariant under $x \mapsto 1 - x$. For $n = 3$ we conclude that one of the parameters, let us say $a_3$, is $\frac{1}{2}$ and $a_1 = 1 - a_2$. Now, restricted to $a_3 = b_3 = \frac{1}{2}$ we have the primary decomposition:

$$I_{3,5} = \langle a_2 - b_1, a_1 - b_2 \rangle \cap \langle a_2 - b_1, a_1 - b_2 \rangle \cap \langle b_2 - 1, a_2 + b_1 - 1, a_1 - 1 \rangle \cap$$

$$\langle b_2 - 1, a_2 - 1, a_1 - b_1 - 1 \rangle \cap \langle b_1 - 1, a_2 - b_1 - 1, a_1 - 1 \rangle \cap \langle b_1 - 1, a_2 - 1, a_1 + b_2 - 1 \rangle$$

This proves Conjecture 3 in this particular case. Note that we use the fact that none of parameters is 1.

For $n = 4$, in a similar way, we can assume that $a_3 = 1 - a_1$ and $a_4 = 1 - a_2$. Again we do not get the primary decomposition of $I_{4,4}$ restricted to the parameters $a_3 = 1 - a_1$, $a_4 = 1 - a_2$, $b_3 = 1 - b_1$, $b_4 = 1 - b_2$. We further use the structure of $\delta_p$ in order to reduce the number of variables so that we can compute the primary decomposition of $I_{4,4}$.

For $q = 2$ or 3 fixed, let us consider the case in which $q$ does not appear in the denominators of $a_i$'s. Using Proposition 1 item 2, we take primes $p$ such that $\delta_p(a_1) = qa_1 - i$ and $\delta_p(a_2) = qa_2 - j$, where $i, j$ are some integers between 0 and $q - 1$.

Lemma 7. For $q = 2, 3$ and $i, j = 0, 1, \ldots, q - 1$, the conjecture 3 is true for $n = 4$ and

$$a_3 = 1 - a_1, a_4 = 1 - a_2,$$

$$b_1 = qa_1 - i, b_2 = qa_2 - j, b_3 = 1 - b_1, b_4 = 1 - b_2$$

In each case the variety $V(I_{4,4})$ is a point with rational coordinates and if we take $0 < a_i \leq \frac{1}{2}$ then we get 7 of 14-hypergeometric cases.

Proof. The proof is purely computational. For $q = 2$ or 3 we have considered $q^2$ cases. In each case, we find that the variety $V(I_{4,4})$ consists only of one point. It has rational coordinates. If we assume that $0 < a_i \leq \frac{1}{2}$ then for $q = 2$ we have only the solutions $(a_1, a_2) = (\frac{1}{2}, \frac{2}{3}), (\frac{1}{2}, \frac{1}{3})$. For $q = 3$ we get

$$(a_1, a_2) = (\frac{1}{2}, \frac{1}{2}), (\frac{1}{4}, \frac{1}{2}), (\frac{1}{4}, \frac{1}{4}), (\frac{1}{8}, \frac{2}{5}), (\frac{1}{8}, \frac{3}{5}), (\frac{1}{10}, \frac{3}{10}).$$

Now, let us assume that 2 and 3 appears in the denominators of $a_i$'s. We are going to use Proposition 1 item 4 for $q = 2, 3$ and $m = 1$. For $q = 2$, we take primes $p$ such that $\delta_p(a_i) = a_i + r_i$, $i = 1, 2$, where $\{r_1, r_2\} \subset \{0, \frac{1}{2}, -\frac{1}{2}\}$. In a similar way, for $q = 3$ we take primes $p$ such that $\delta_p(a_i) = a_i + s_i$, $i = 1, 2$, where $\{s_1, s_2\} \subset \{0, \frac{1}{2}, -\frac{1}{2}, \frac{2}{5}, -\frac{2}{5}, -\frac{3}{5}, \frac{3}{5}\}$. We can assume that $r_1$ and $r_2$ (resp. $s_1$ and $s_2$) are not simultaneously zero. Let $I_{4,4,2,r_1,r_2}$, be $I_{4,4}$ restricted to the parameters:

$$a_3 = 1 - a_1, a_4 = 1 - a_2.$$
Moreover, it has rational coordinates. If we put the condition $0 < a_i \leq \frac{1}{2}$ we get the remaining 7 examples in the list (1).

3.4 Computational evidence for conjectures 1 and 2

For $n = 2$ and $\{a_1, a_2\} = \{\frac{1}{2}(1 \pm \frac{1}{m_1} - \frac{1}{m_2})\}$ with $m_1, m_2 \in \mathbb{N}$ and $\frac{1}{m_1} + \frac{1}{m_2} > 1$ the monodromy group of (1) is a triangle group of type $(m_1, m_2, \infty)$ and we have checked the Conjecture 1 for the truncated $q(a|z)$ (mod $q^{182}$) and for all the cases

$$m_1 \leq m_2 \leq 24, \text{ or } m_1 \leq 24, m_2 = \infty.$$ 

and primes $2 \leq p \leq 181$. For more computation of this type see the first author’s homepage. For Conjecture 3 (which implies Conjecture 2), apart from its verification in particular cases done in §3, we have checked it for many other special loci in the parameter space $a, b$. The strategy is always to reduce the number of variables so that we can compute the primary decomposition of $I_{n,m}$ by a computer. The detailed discussion of this topic will be written somewhere else.

3.5 Proof of Corollary 1

Corollary 1 follows from Theorem 1, part 2 for $n = 4$ and

Proposition 2. We have $u_i(Nz) \in \mathbb{Z}[[z]], i = 0, 1, \ldots, 6$.

Proof. We prove that for any prime $p$, $u_i(Nz)$ is $p$-integral. Let $a_i = \frac{r_i}{s_i}, (r_i, s_i) = 1$. For some $a_i$ such that $p$ does not divide $s_i$, by Lemma (3) $(a_i)_k$ is $p$-integral. Let us assume that $p|s_i$ for some $a_i$. For each $(a_i)_k$ we need to multiply it with $p^{k-\text{ord}_p s_i}$ in order to make it $p$-integral. By the equality (14), $\frac{k^j \cdot s_i}{(k!p)^j}$ is $p$-integral. All these together imply that $u_1(N_p z)$ and so all $\theta^i u_1$, $i = 1, 2, 3, 4$, are $p$-integral.

For $u_5$ we proceed as follows. Since $u_1(Nz) \in 1 + z \cdot \mathbb{Z}[[z]]$, it is enough to prove the statement for $W(a|z) := \frac{u_5(z)}{u_1(z)^2} = \theta^5_P$ (here we need to emphasize that $u_i$’s depend on $a$). Acting $\theta$ on the both sides of the congruence in Theorem 4 we get $W(\delta_p(a)|N_p z^p) - W(a|N_p z) \in \mathbb{Z}_p[[z]]$ which implies that $W(a|N_p z) \in \mathbb{Z}_p[[z]]$. \hfill $\square$

The most important modular object arising from the periods of Calabi-Yau varieties is the Yukawa coupling:

$$Y := n_0 \frac{u_1^4}{(u_5 + u_1^2)^3(1 - z)} = n_0 + \sum_{d=1}^{\infty} n_d d^3 \frac{q^d}{1-q^d}.$$ 

Here, $n_0 := \int_M \omega^3$, where $M$ is the A-model Calabi-Yau threefold of mirror symmetry and $\omega$ is the Kähler form (the Picard-Fuchs equation (1) is satisfied by the periods of B-model Calabi-Yau threefold). The numbers $n_d$ are supposed to count the number of rational curves of degree $d$ in a generic $M$. For the case $a_i = \frac{1}{5}, i = 1, 2, 3, 4$ few coefficients $n_d$ are given by $n_d = 5, 2875, 609250, 317206375, \cdots$. 

13
References


