Ann. Math. Québec (2015) 39:185–203
DOI 10.1007/s40316-015-0031-9

Dwork congruences and reflexive polytopes

Kira Samol[1] · **Duco van Straten**[1]

Received: 4 September 2014 / Accepted: 8 April 2015 / Published online: 11 August 2015

Abstract We show that the coefficients of the power series expansion of the principal period of a Laurent polynomial satisfy strong congruence properties. These congruences play key role in the explicit p-adic analytic continuation of the unit-root. The methods we use are completely elementary.

Résumé Nous montrons que les coefficients du développement en série de puissances de la période principale d'un polynôme de Laurent satisfont à de fortes propriétés de congruence. Ces congruences jouent un rôle clé pour le prolongement analytique p-adique explicite sur le disque unité.

Keywords Laurent polynomials · Dwork congruences · Analytic continuation · Newton polyhedrons · Polytopes

Mathematics Subject Classification 11K31 · 11B99 · 14J33

1 Introduction

The sequence of numbers

$$a(0), a(1), a(2), a(3), \ldots = 1, 3, 19, 147, \ldots$$

with general term

$$a(n) = \sum_{k=0}^{\infty} \binom{n}{k}^2 \binom{n+k}{k}$$

played a crucial role in Apéry's irrationality proof [2] of $\zeta(2)$. These numbers satisfy various remarkable congruence properties [3,4], like

✉ Duco van Straten
straten@mathematik.uni-mainz.de

1 Institut für Mathematik, FB 08 Physik, Mathematik und Informatik, Johannes Gutenberg-Universität, 55099 Mainz, Germany

$$a(mp^r - 1) \equiv a(mp^{r-1} - 1) \mod p^{3r}$$

for a prime p and m a number prime to p.

Another simple property is the following: when we write the number n in base p as

$$n = n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r$$

with $0 \le n_i \le p - 1$, then

$$a(n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r) \equiv a(n_0)a(n_1)a(n_2)\cdots a(n_r) \mod p.$$

This is a consequence of more general congruences that we call *Dwork congruences* and which were used by Dwork for the p-adic analytic continuation of the associated *period function*

$$\Phi(t) = \sum_{n=0}^{\infty} a(n)t^n$$

that satisfies the Picard–Fuchs equation

$$(\theta^2 - t(11\theta^2 + 11\theta + 3) - t^2(\theta + 1)^2)\Phi(t) = 0$$

where $\theta = t\partial/\partial t$.

In this paper, we show that these Dwork congruences result from the fact that the coefficient $a(n)$ is the constant term of the nth power of a Laurent polynomial, whose Newton-polytope has *a unique interior point*. The sequence of Apéry numbers can be generated in that way, as one can take for example

$$f(x, y) = 3 + x + y + 2\left(\frac{1}{x} + \frac{1}{y}\right) + \frac{x}{y} + \frac{y}{x} + \frac{1}{xy}$$

and one has

$$a(n) = \text{constant term of } f^n$$

2 Dwork congruences

Definition 2.1 Let $\{a(n)\}_{n\in\mathbb{N}_0}$ be a sequence of integers with $a(0) = 1$ and let p be a prime number. We say that $\{a(n)\}_n$ satisfies the *Dwork congruences* if for all $s, m, n \in \mathbb{N}_0$ one has

(D1) $\dfrac{a(n)}{a(\lfloor n/p \rfloor)} \in \mathbb{Z}_p$,

(D2) $\dfrac{a(n + mp^{s+1})}{a(\lfloor n/p \rfloor + mp^s)} \equiv \dfrac{a(n)}{a(\lfloor n/p \rfloor)} \mod p^{s+1}$.

In fact, the validity of these congruences is implied by those for which $n < p^{s+1}$, as one sees by writing $n = n' + mp^{s+1}$ with $n' < p^{s+1}$. By cross-multiplication, (D2) becomes

(D3) $a(n + mp^{s+1})a(\lfloor \frac{n}{p} \rfloor) \equiv a(n)a(\lfloor \frac{n}{p} \rfloor + mp^s) \mod p^{s+1}$.

The congruences for $s = 0$ say that for $0 \le n_0 \le p - 1$ one has

$$a(n_0 + mp) \equiv a(n_0)a(m) \mod p.$$

So if we write n in base p as

$$n = n_0 + pn_1 + \cdots + n_r p^r, \quad 0 \le n_i \le p - 1,$$

we find by repeated application that

$$a(n) \equiv a(n_0)a(n_1)\cdots a(n_r) \mod p.$$

In fact, this is easily seen to be equivalent to D3 for $s = 0$.

Similarly, for higher s the congruences D3 are equivalent to

$$\begin{aligned} &a(n_0 + \cdots + n_{s+1}p^{s+1})a(n_1 + \cdots + n_s p^{s-1}) \\ &\quad \equiv a(n_0 + \cdots + n_s p^s)a(n_1 + \cdots + n_{s+1}p^s) \mod p^{s+1}. \end{aligned} \tag{2.1}$$

The congruences express a strong p-adic analyticity property of the function

$$n \longmapsto \frac{a(n)}{a(\lfloor n/p \rfloor)}$$

and play a key role in the p-adic analytic continuation of the series

$$F(t) = \sum_{n=0}^{\infty} a(n)t^n$$

to points on the closed p-adic unit disc. More precisely, one has the following theorem (see [8, Theorem 3]).

Theorem 2.2 *Let* $\{a(n)\}_n$ *be a* $\mathbb{Z}_p$*-valued sequence satisfying the Dwork congruences* D1 *and* D2. *Let*

$$F(t) = \sum_{n=0}^{\infty} a(n)t^n \quad \text{and} \quad F^s(t) = \sum_{n=0}^{p^s-1} a(n)t^n.$$

Let $\mathfrak{D}$ *be the region in* $\mathbb{Z}_p$ *defined by*

$$\mathfrak{D} := \{x \in \mathbb{Z}_p \colon |F^1(x)| = 1\}.$$

Then $\frac{F(t)}{F(t^p)}$ *is the restriction to* $p\mathbb{Z}_p$ *of an analytic element* f *of support* $\mathfrak{D}$:

$$f(x) = \lim_{s\to\infty} \frac{F^{s+1}(x)}{F^s(x^p)}.$$

The congruences were used in [10] to determine Frobenius polynomials associated to Calabi–Yau motives coming from fourth order operators of Calabi–Yau type from the list [1]. Although there are many examples of sequences that satisfy these congruences, the true cohomological meaning remains obscure at present. For a recent interpretation in terms of formal groups, see [11]. In this paper we will give a completely elementary proof of the congruences D3 for sequences $\{a(n)\}_n$ that arise as constant term of the powers of a fixed Laurent polynomial with integral coefficients and whose Newton polyhedron contains a unique interior point. These include the series that come from reflexive polytopes.

3 Laurent polynomials

We will use the familiar multi-index notation for monomials and exponents

$$X^{\mathbf{a}} = X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}, \quad \mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n,$$

to write a general Laurent polynomial as

$$f=\sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}} \in \mathbb{Z}\left[X_1, X_1^{-1}, X_2, X_2^{-1}, \ldots, X_n, X_n^{-1}\right].$$

The *support* of f is the set of exponents $\mathbf{a}$ occuring in f, i.e.,

$$\operatorname{supp}(f) := \{\mathbf{a} \in \mathbb{Z}^n \mid c_{\mathbf{a}} \neq 0\}.$$

The *Newton polyhedron* $\Delta(f) \subset \mathbb{R}^n$ of f is defined as the convex hull of its support, namely

$$\Delta(f) := \operatorname{convex}(\operatorname{supp}(f)).$$

When the support of f consists of m monomials, we can put the information of the polyhedron $\Delta := \Delta(f)$ in an $n \times m$ matrix $\mathcal{A} \in Mat(m \times n, \mathbb{Z})$, whose columns $\mathbf{a}_j$, $j = 1, 2, \ldots, m$, are the exponents of f,

$$\mathcal{A}=(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m)=\begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,m} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,m} \\ \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,m} \end{pmatrix},$$

so that we can write

$$f=\sum_{j=1}^{m} c_j X^{\mathbf{a}_j}=\sum_{j=1}^{m} c_j \prod_{i=1}^{n} X^{a_{i,j}}.$$

The polyhedron Δ is the image of the standard simplex Δ_m under the map

$$\mathbb{R}^m \xrightarrow{\mathcal{A}} \mathbb{R}^n.$$

The following theorem will play a key role in the sequel.

Theorem 3.1 *Let Δ be an integral polyhedron with 0 as unique interior point. Then for all non-negative integral vectors $(\ell_1, \ell_2, \ldots, \ell_m) \in \mathbb{Z}^m$ such that $\sum_{i=1}^m a_{i,j}\ell_j \neq 0$ for some $1 \leq i \leq n$, one has*

$$\gcd_{i=1,\ldots,n}\left(\sum_{j=1}^{m} a_{i,j}\ell_j\right) \leq \sum_{j=1}^{m} \ell_j.$$

Proof Assume that there exists a non-negative integral vector $\ell = (\ell_1, \ldots, \ell_m) \in \mathbb{Z}^m$ such that $\sum_{i=1}^m a_{i,j}\ell_j \neq 0$ for some $1 \leq i \leq n$ and

$$\gcd_{i=1,\ldots,n}\left(\sum_{j=1}^{m} a_{i,j}\ell_j\right) > \sum_{j=1}^{m} \ell_j.$$

We have

$$\mathbf{a}_1\ell_1+\cdots+\mathbf{a}_m\ell_m=\mathcal{A}\begin{pmatrix} \ell_1 \\ \vdots \\ \ell_m \end{pmatrix}=\begin{pmatrix} \sum_{j=1}^{m} a_{1,j}\ell_j \\ \vdots \\ \sum_{j=1}^{m} a_{n,j}\ell_j \end{pmatrix}.$$

The components of the vector at the right-hand side are all divisible by g, so that after division by g we obtain a non-zero lattice point

$$v := \frac{\ell_1}{g}\mathbf{a}_1 + \cdots + \frac{\ell_m}{g}\mathbf{a}_m \in \mathbb{Z}^n$$

of Δ with

$$\sum_j \frac{\ell_j}{g} < 1.$$

The interior points of Δ (i.e., the points that do not lie on the boundary) consist of the combinations

$$\alpha_1\mathbf{a}_1 + \cdots + \alpha_m\mathbf{a}_m$$

of the columns of $\mathcal{A}$ with $\sum_{j=1}^m \alpha_j < 1$. As 0 was assumed to be the only interior lattice point of Δ we arrive at a contradiction. □

We remark that the above statement applies in particular to *reflexive polyhedra*.

4 The fundamental period

Notation 4.1 *For a Laurent polynomial we denote by* $[f]_0$ *the* constant term*, that is, the coefficient of the monomial* X^0.

Definition 4.2 The *fundamental period* of f is the series

$$\Phi(t) := \sum_{k=0}^{\infty} a(k)t^k, \quad a(k) := [f^k]_0.$$

Note that the function $\Phi(t)$ can be interpreted as the period of a holomorphic differential form on the hypersurface

$$X_t := \{t.f = 1\} \subset (\mathbb{C}^*)^n,$$

as one has

$$\Phi(t) = \sum_{k=0}^{\infty}[f^k]_0 t^k = \sum_{k=0}^{\infty} \frac{1}{(2\pi i)^n}\int_T f^k t^k \Omega$$
$$= \frac{1}{(2\pi i)^n}\int_T \sum_{k=0}^{\infty} f^k t^k \Omega = \frac{1}{(2\pi i)^n}\int_T \frac{1}{1-tf}\Omega = \int_{\gamma_t} \omega_t.$$

Here

$$\Omega := \frac{dX_1}{X_1}\frac{dX_2}{X_2}\cdots\frac{dX_n}{X_n},$$

T is the cycle given by $|X_i| = \epsilon_i$ and homologous to the Leray coboundary of $\gamma_t \in H_{n-1}(X_t)$ and

$$\omega_t = Res_{X_t}\left(\frac{1}{1-tf}\Omega\right)$$

In particular, $\Phi(t)$ is a solution of a Picard–Fuchs equation; the coefficients $a(k)$ satisfy a linear recursion relation.

Theorem 4.3 *Let $f \in \mathbb{Z}[X_1, X_1^{-1}, \dots, X_n, X_n^{-1}]$ with integral coefficients. Assume that the Newton polyhedron $\Delta(f)$ has 0 as its unique interior lattice point. Then the coefficients $a(n) = [f^n]_0$ of the fundamental period satisfy for each prime number p and $s \in \mathbb{N}$ the congruence*

$$\begin{aligned} &a(n_0 + \cdots + n_s p^s) a(n_1 + \cdots + n_{s-1} p^{s-2}) \\ &\quad \equiv a(n_0 + \cdots + n_{s-1} p^{s-1}) a(n_1 + \cdots + n_s p^{s-1}) \mod p^s, \end{aligned} \tag{4.1}$$

where $0 \le n_i \le p-1$ for $0 \le i \le s-1$.

We remark that already for the simplest cases where the the Newton polyhedron contains more than one lattice point, like $f = X^2 + X^{-1}$, the coefficients $a(n)$ do not satisfy such simple congruences.

5 Proof for the congruence mod p

For $s = 1$ we have to show that for all $n_0 \le p - 1$,

$$a(n_0 + n_1 p) \equiv a(n_0) a(n_1) \mod p\,.$$

The proof we will give is completely elementary; the key ingredient is Theorem 3.1, which states that for all non-negative integral $\ell = (\ell_1, \dots, \ell_m)$, one has

$$\gcd_{i=1,\dots,n} \left(\sum_{j=1}^m a_{i,j} \ell_j \right) \le \sum_{j=1}^m \ell_j .$$

Proposition 5.1 *Let f be a Laurent polynomial as above and $n_0 < p$. Then*

$$\left[f^{n_0} f^{n_1 p}\right]_0 \equiv \left[f^{n_0}\right]_0 \left[f^{n_1}\right]_0 \mod p.$$

Proof As f has integral coefficients, we have $f^{n_1 p}(X) \equiv f^{n_1}(X^p) \mod p$. So the congruence is implied by the equality

$$\left[f^{n_0}(X) f^{n_1}(X^p)\right]_0 = \left[f^{n_0}(X)\right]_0 \left[f^{n_1}(X)\right]_0 ,$$

which means: the product of a monomial from $f^{n_0}(X)$ and a monomial from $f^{n_1}(X^p)$ can never be constant, unless the two monomials are constant themselves. It is this statement that we will prove now.

For the product of a non-constant monomial from $f^{n_0}(X)$ and a non-constant monomial from $f^{n_1}(X^p)$ to be constant, the monomial coming from $f^{n_0}(X)$ has to be a monomial in $X_1^p, \dots, X_n^p$, since all monomials in $f^{n_1}(X^p)$ are monomials in $X_1^p, \dots, X_n^p$.

A monomial

$$M := X^{\ell_1 \mathbf{a}_1 + \ell_2 \mathbf{a}_2 + \cdots + \ell_m \mathbf{a}_m} = \prod_{j=1}^m X_1^{a_{1,j}\ell_j} \cdots X_n^{a_{n,j}\ell_j}$$

appearing in $f^{n_0}(X)$ corresponds to a partition

$$n_0 = \ell_1 + \cdots + \ell_m$$

of n_0 in non-negative integers ℓ_i. On the one hand, if M were a monomial in $X_1^p, \ldots, X_n^p$, then we would have the divisibility

$$p \,\Big|\, \sum_{j=1}^{m} a_{i,j}\, \ell_j \quad \text{for } 1 \le i \le n,$$

and hence

$$p \,\Big|\, \gcd_{i=1,\ldots,n} \left(\sum_{j=1}^{m} a_{i,j} \ell_j \right).$$

On the other hand, by 3.1 we have

$$\gcd_{i=1,\ldots,n} \left(\sum_{j=1}^{m} a_{i,j} \ell_j \right) \le \sum_{j=1}^{m} \ell_j = n_0 < p.$$

So we conclude that

$$\sum_{i=1}^{m} a_{i,j} \ell_j = 0 \quad \text{for } 1 \le j \le n$$

and that the monomial M is the constant monomial X^0. Hence it follows that

$$\left[f^{n_0}(X) f^{n_1}(X^p) \right]_0 = \left[f^{n_0}(X) \right]_0 \left[f^{n_1}(X^p) \right]_0,$$

and since

$$\left[f^{n_1}(X^p) \right]_0 = \left[f^{n_1}(X) \right]_0,$$

the proposition follows. $\square$

We remark that the congruence has the following interpretation. By a result of [7] (Theorem 4.) one can compactify the map $f\colon (\mathbb{C}^*)^n \longrightarrow \mathbb{C}$ given by the Laurent polynomial to a map $\phi\colon \mathcal{X} \longrightarrow \mathbb{P}^1$ such that the differential form Ω extends to a form in $\Omega^n((\mathcal{X} \backslash \phi^{-1}(\{\infty\})))$. In the case $\Delta(f)$ is reflexive one has

$$\deg(\pi_* \omega_{X/S}) = 1;$$

see (8.3) of [6]. On the other hand, from this and under an additional condition (R), it follows from Corollary 3.7 of [11] that the $\mod p$ Dwork-congruences hold.

6 Strategy for higher *s*

The idea for the higher congruences is basically the *same as for* $s = 1$, but is combinatorially more involved. Surprisingly, one does not need any statements stronger than 3.1. To prove the congruence 4.1, we have to show that

$$\left[\prod_{k=0}^{s} f^{n_k p^k} \right]_0 \left[\prod_{k=1}^{s-1} f^{n_k p^{k-1}} \right]_0 \equiv \left[\prod_{k=0}^{s-1} f^{n_k p^k} \right]_0 \left[\prod_{k=1}^{s} f^{n_k p^{k-1}} \right]_0 \mod p^s. \tag{6.1}$$

To do this, we will use the following expansion of $f^{np^s}(X)$.

Proposition 6.1 *We can write*

$$f^{np^s}(X)=\sum_{k=0}^{s}p^k g_{n,k}(X^{p^{s-k}}),$$

where $g_{n,k}$ is a polynomial of degree np^k in the monomials of f, independent of s, defined inductively by $g_{n,0}(X)=f^n(X)$ and

$$p^k g_{n,k}(X):=f(X)^{np^k}-\sum_{j=0}^{k-1}p^j g_{n,j}(X^{p^{k-1-j}}). \tag{6.2}$$

Proof We have to prove that the right-hand side of Eq. 6.2 is divisible by p^k. This is proved by induction on k and an application of the congruence

$$f(X)^{p^m}\equiv f(X^p)^{p^{m-1}} \mod p^m. \tag{6.3}$$

For $k=1$, the divisibility follows directly by (6.3). Assume that the statement is true for $m\le k-1$. Write

$$f(X)^{np^{k-1}}=\sum_{j=0}^{k-1}p^j g_{n,j}(X^{p^{k-1-j}}).$$

Then,

$$\sum_{j=0}^{k-1}p^j g_{n,j}(X^{p^{k-j}})=f(X^p)^{np^{k-1}}\equiv f(X)^{np^k} \mod p^n,$$

and thus

$$f(X)^{np^k}-\sum_{j=0}^{k-1}p^j g_{n,j}(X^{p^{k-j}})\equiv 0 \mod p^n.$$

$\square$

The congruences involve constant term expressions of the form

$$\begin{aligned}\left[\prod_{k=a}^{b}f^{n_k p^k}\right]_0&=\left[\prod_{k=a}^{b}\sum_{j=0}^{k}p^j g_{n_k,j}(X^{p^{k-j}})\right]_0\\&=\sum_{i_a\le a}\cdots\sum_{i_b\le b}p^{\sum_{k=a}^{b}i_k}\left[\prod_{k=a}^{b}g_{n_k,i_k}(X^{p^{k-i_k}})\right]_0.\end{aligned} \tag{6.4}$$

Thus, Eq. (6.1) translates modulo p^s into

$$\begin{aligned}&\sum_{i_0\le 0}\cdots\sum_{i_s\le s}\sum_{j_1\le 0}\cdots\sum_{j_{s-1}\le s-2}p^A\left[\prod_{k=0}^{s}g_{n_k,i_k}\left(X^{p^{k-i_k}}\right)\right]_0\left[\prod_{k=1}^{s-1}g_{n_k,j_k}\left(X^{p^{k-1-j_k}}\right)\right]_0\\&\equiv\sum_{i_0\le 0}\cdots\sum_{i_{s-1}\le s-1}\sum_{j_1\le 0}\cdots\sum_{j_s\le s-1}p^B\left[\prod_{k=0}^{s-1}g_{n_k,i_k}\left(X^{p^{k-i_k}}\right)\right]_0\left[\prod_{k=1}^{s}g_{n_k,j_k}\left(X^{p^{k-1-j_k}}\right)\right]_0\end{aligned} \tag{6.5}$$

with

$$A := \sum_{k=0}^{s} i_k + \sum_{k=1}^{s-1} j_k \quad \text{and} \quad B := \sum_{k=0}^{s-1} i_k + \sum_{k=1}^{s} j_k.$$

Since this congruence is supposed to hold modulo p^s, on the left-hand side, only the summands in A with

$$\sum_{k=0}^{s} i_k + \sum_{k=1}^{s-1} l_k \leq s-1$$

contribute, and on the right-hand side, only those in B with

$$\sum_{k=0}^{s-1} i_k + \sum_{k=1}^{s} l_k \leq s-1$$

play a role.

Now, we proceed by comparing these summands on both sides of Eq. 6.1. We will prove that each summand on the right-hand side is equal to exactly one summand on the left-hand side and vice versa.

7 Splitting positions

So we are led to study for $a \leq b$ expressions of the type

$$G(a,b;I) := \left[\prod_{k=a}^{b} g_{n_k,i_k}\left(X^{p^{k-i_k}}\right)\right]_0$$

where the integers $0 \leq n_k \leq p-1$ are fixed for $a \leq k \leq b$ and $I := (i_a, \ldots, i_b)$ is a sequence with $0 \leq i_k \leq k$.

Definition 7.1 We say that $G(a,b;I)$ *splits at* ℓ if

$$G(a,b;I) = G(a,\ell-1;I)\, G(\ell,b;I).$$

The number of entries of I is determined implicitly by a and b, so that by the product $G(a,\ell-1;I)$ we mean the expression corresponding to the sequence $(i_a,\ldots,i_{\ell-1})$, while by $G(\ell,b;I)$, we mean the expression corresponding to $(i_\ell,\ldots,i_b)$. Note that $\ell = a$ represents a trivial splitting, but splitting at $\ell = b$ is a non-trivial property.

Proposition 7.2 *If $k - i_k \geq \ell$ for all $k \geq \ell$, then $G(a,b;I)$ splits at ℓ.*

Proof A monomial $\prod_{j=1}^{m}(X^{p^{k-i_k}})^{\mathbf{a}_j\beta_{j,k}}$ occuring in $g_{n_k,i_k}(X^{p^{k-i_k}})$ corresponds to a partition

$$\beta_{1,k} + \cdots + \beta_{m,k} = p^{i_k} n_k \leq p^{i_k+1} - p^{i_k}$$

of the number $p^{i_k} n_k$ in non-negative integers $\beta_{1,k}, \ldots, \beta_{m,k}$. So we have

$$p^{k-i_k}(\beta_{1,k} + \cdots + \beta_{m,k} \leq p^{k+1} - p^k.$$

It follows from the assumptions that the product

$$G(\ell, b; I) = \prod_{k=\ell}^{b} g_{n_k,i_k}\big(X^{p^{k-i_k}}\big)$$

is a Laurent polynomial in X^p. As a consequence, the product of a monomial in

$$G(a, \ell-1; I) = \prod_{k=a}^{\ell-1} g_{n_k,i_k}(X^{p^{k-i_k}})$$

and a monomial of $G(\ell, b; I)$ can be constant only if the sum

$$m_i := \sum_{j=1}^{m} p^{a-i_a} a_{i,j}\beta_{j,a} + \cdots + \sum_{j=1}^{m} p^{\ell-1-i_{\ell-1}} a_{i,j}\beta_{j,\ell-1}$$

is divisible by p^ℓ for $1 \leq i \leq n$.

Set

$$\gamma_j := p^{a-i_a}\beta_{j,a} + \cdots + p^{\ell-1-i_{\ell-1}}\beta_{j,\ell-1}$$

so that

$$\sum_{j=1}^{m} a_{i,j}\gamma_j = m_i.$$

It follows that

$$\begin{aligned}\sum_{j=1}^{m}\gamma_j &= \sum_{j=1}^{m} p^{a-i_a}\beta_{j,a} + \cdots + \sum_{j=1}^{m} p^{\ell-1-i_{\ell-1}}\beta_{j,\ell-1}\\ &\leq p^{a+1} - p^a + \cdots + p^\ell - p^{\ell-1} = p^\ell - p^a < p^\ell.\end{aligned}$$

Hence, it follows that

$$p^\ell \;\Bigg|\; \gcd_{i=1,\ldots,n}\left(\sum_{j=1}^{m} a_{i,j}\gamma_j\right) \leq \sum_{j=1}^{m}\gamma_j < p^\ell,$$

where the first inequality follows from Theorem 3.1. This implies

$$\sum_{j=1}^{m} a_{i,j}\gamma_j = 0 \quad \text{for } 1 \leq i \leq n.$$

But this means that the monomial in

$$\prod_{k=t}^{s-1} g_{n_k,i_k}\big(X^{p^{k-i_k}}\big)$$

is itself constant. □

Now that we know that we can split up expressions $G(a, b; I)$ satisfying the condition given in Proposition 7.2, we proceed by proving that all the summands on both sides of Eq. 6.5 that do not have a coefficient divisible by p^s satisfy this splitting condition.

8 Three combinatorial lemmas

In this section, we prove three simple combinatorial lemmas which will be applied to split up expressions $G(0, s; I)\, G(1, s-1; J+1)$ that occur in the congruence (6.1).

Definition 8.1 Let $a \le b$ and $I = (i_a, i_{a+1}, \ldots, i_b)$ a sequence with $0 \le i_k \le k$ for all k with $a \le k \le b$. We say that ℓ is a *splitting index for* I if $\ell > a$ and for $k \ge \ell$ one has $i_k \le k - \ell$.

Remark that for a splitting index ℓ one can apply 7.2 and that $i_\ell = 0$.

Lemma 8.2 *Let I as above and assume that*

$$\sum_{k=a}^{b} i_k \le b - a - 1.$$

Then there exists at least one splitting index for I.

Proof Let

$$\mathcal{N} := \{k \mid i_k = 0\}$$

be the set of all indices k such that the corresponding i_k is zero. Since the sum has $b-a+1$ summands i_k, the set $\mathcal{N}$ has at least two elements. So there exists at least one index $k \neq a$ such that $i_k = 0$. We will show by contradiction that one of these zero-indices is a splitting index.

We say that $\nu > k$ is a *violating index* with respect to $k \in \mathcal{N}$ if $i_\nu > \nu - k$. Assume now that all $k \in \mathcal{N}$ posses a violating index. It follows directly that for each violating index ν, $i_\nu \ge 2$. Furthermore, if ν is a violating index for m different zero-indices $k_1 < \cdots < k_m$, it follows that $i_\nu \ge m + 1$.

Now assume that we have μ different violating indices $\nu_1, \ldots, \nu_\mu$ and that ν_j is a violating index for all $j \in \mathcal{N}_j$, where we partition $\mathcal{N}$ into disjoint subsets

$$\mathcal{N} = \mathcal{N}_1 \cup \mathcal{N}_2 \cup \cdots \cup \mathcal{N}_\mu.$$

Then

$$\sum_{j=1}^{\mu} i_{\nu_j} \ge \sum_{j=1}^{\mu} (\#\mathcal{N}_j + 1) = \#\mathcal{N} + \mu,$$

and

$$\sum_{k=a+1}^{b} i_k \ge \#\mathcal{N} \cdot 0 + \sum_{j=1}^{\mu} i_{\nu_j} + (b - a - (\#\mathcal{N} + \mu)) \cdot 1 = b - a > b - a - 1,$$

a contradiction. □

We can sharpen Lemma 8.2 to the following one.

Lemma 8.3 *Let I be as above and assume that*

$$\sum_{k=a}^{b} i_k = b - a - m.$$

Then there exist at least m different splitting indices for I.

Proof We proceed by induction on m. The case $m = 1$ is just Lemma 8.2. Assume that for all $n \leq m$, we have proven the statement. Now assume

$$\sum_{k=a}^{b} i_k = b - a - (m+1).$$

Since $m + 1 > 1$, there exists a splitting index ν. We can split up the set of indices

$$\{i_a, \ldots, i_b\} = \{i_a, \ldots, i_{\nu-1}\} \cup \{i_\nu, \ldots, i_b\}$$

in position ν such that

$$\sum_{k=a}^{\nu-1} i_k = N_\nu \quad \text{and} \quad \sum_{k=\nu}^{b} i_k = b - a - m - 1 - N_\nu.$$

Depending on N_ν, we have to distinguish between the following cases.

Case (1): $N_\nu > (\nu - 1) - a - 1$. It follows that

$$b - a - m - 1 - N_\nu < b - a - m - ((\nu - 1) - a - 1) = b - m - (\nu - 1),$$

and thus

$$\sum_{k=\nu}^{b} i_k \leq b - \nu - m.$$

By induction, there exists at least m splitting indices in $(i_\nu, \ldots, i_b)$, and thus for the whole $(i_a, \ldots, i_b)$, there exist at least $m + 1$ such indices.

Case (2): The case $N_\nu \leq (\nu - 1) - a - 1$ splits up in two subcases:

(i) $N_\nu \leq (\nu - 1) - a - m$. By induction, $(i_a, \ldots, i_{\nu-1})$ has at least m splitting indices, and the whole $(i_a, \ldots, i_b)$ has at least $m + 1$ such indices.

(ii) $N_\nu = (\nu - 1) - a - n$, where $1 \leq n \leq m$. Since

$$\sum_{k=a}^{\nu-1} i_k = (\nu - 1) - a - n,$$

by induction for $(i_a, \ldots, i_{\nu-1})$ there exist at least n splitting indices. Since

$$\sum_{k=\nu}^{b} i_k = b - \nu - (m - n),$$

for $(i_\nu, \ldots, i_b)$, there exist at least $m-n$ splitting indices. Thus, for the whole $(i_a, \ldots, i_b)$ there exist at least $n + (m - n) + 1 = m + 1$ splitting indices. □

Lemma 8.4 (i) *Let* $I = (i_0, \ldots, i_s)$ *and* $J = (j_1, \ldots, j_{s-1})$ *with*

$$\sum_{k=0}^{s} i_k + \sum_{k=1}^{s-1} j_k \leq s - 1.$$

Let S_I *be the set of splitting indices of* I *and* S_J *be the set of splitting indices of* J*. Then,*

$$S_I \cap (S_J \cup \{1, s\}) \neq \emptyset.$$

(ii) *Let* $I = \{i_0, \dots, i_{s-1}\}$ *and* $J = (j_1, \dots, j_s)$ *with*

$$\sum_{k=0}^{s-1} i_k + \sum_{k=1}^{s} j_k \leq s - 1.$$

Let S_I *be the set of splitting indices of* I *and* S_J *be the set of splitting indices of* J*. Then,*

$$(S_I \cup \{s\}) \cap (S_J \cup \{1\}) \neq \emptyset.$$

Proof (i) Since $S_I \cup S_J \cup \{1, s\} \subset \{1, 2, \dots, s\}$, it follows that

$$\#(S_I \cup S_J \cup \{1, s\}) \leq s.$$

Note that

$$\sum_{k=0}^{s} i_k \geq s - \#S_I$$

by Lemma 8.3. This implies that

$$\sum_{k=1}^{s-1} j_k \leq s - 2 - (s - (\#S_I + 1)),$$

and hence that $\#S_J \geq s - (\#S_I + 1)$ by Lemma 8.3. But

$$\#S_I + \#S_J + 2 = \#S_I + s - (\#S_I + 1) + 2 = s + 1 > s,$$

which implies

$$\#(S_I \cap (S_J \cup \{1, s\})) \geq 1,$$

and thus the statement follows.

(ii) Note that since $(S_I \cup \{s\}) \cup (S_J \cup \{1\}) \subset \{1, \dots, s\}$, it follows that

$$\#(S_I \cup \{s\}) \cup (S_J \cup \{1\}) \leq s.$$

Now

$$\sum_{k=0}^{s-1} i_k \geq s - 1 - \#S_I,$$

which implies

$$\sum_{k=1}^{s} j_k \leq s - 1 - (s - \#S_I - 1) \quad \text{and} \quad \#S_J \geq s - \#S_I - 1.$$

But

$$\#S_I + 1 + \#S_J + 1 \geq \#S_I + 1 + s - \#S_I = s + 1 > s,$$

which implies that

$$\#((S_I \cup \{s\}) \cap (S_J \cup \{1\})) \geq 1,$$

and the statement follows. □

9 Proof for higher s

We will use the combinatorial lemmas on splitting indices from the last section to prove the congruence (6.1) modulo p^s. For a sequence $I = (i_a, \ldots, i_b)$, we write

$$p^I := p^{\sum_{k=a}^{b} i_k}.$$

For a sequence $J = (j_a, \ldots, j_b)$, we define

$$J + 1 := (j_a + 1, \ldots, j_b + 1).$$

Note that if $k - j_k > 0$ for $a \le k \le b$, then we have

$$G(a, b; J + 1) = G(a, b; J), \tag{9.1}$$

since the constant term of a Laurent polynomial $f(X)$ is the same as the constant term of the Laurent polynomial $f(X^p)$.

Let

$$p^{I+J} G(0, s; I)\, G(1, s - 1; J + 1)$$

be a summand on the left-hand side of (6.5) defined by the tuple (I, J) with

$$\sum_{k=0}^{s} i_k + \sum_{k=1}^{s-1} j_k \le s - 1,$$

and let $1 \le \nu \le s$ be such that $G(0, s; I)$ splits in position ν and either $G(1, s - 1; J + 1)$ splits in position ν or $\nu \in \{1, s\}$. We know that such a ν exists by Lemma 8.4.

Define $I' = (i'_0, \ldots, i'_{s-1})$ and $J' = (j'_1, \ldots, j'_s)$ by

$$\begin{cases} i'_k = i_k & \text{for } k \le \nu - 1, \\ i'_k = j_k & \text{for } k \ge \nu, \\ j'_k = j_k & \text{for } k \le \nu - 1, \\ j'_k = i_k & \text{for } k \ge \nu. \end{cases}$$

To show that $p^{I'+J'} G(0, s - 1; I')\, G(1, s; J' + 1)$ is in fact a summand on the right-hand side of (6.5), we have to explain why $i'_k \le k$ and $j'_k \le k - 1$. Note that $j_k \le k - 1$ for $1 \le k \le s - 1$ and $i_k \le k$ for $0 \le k \le s$. Furthermore, we have $i_k \le k - 1$ for $k \ge \nu$ since $i_\nu = 0$ and $G(0, s; I)$ splits in position ν, which means that $k - i_k \ge \nu \ge 1$ for $k \ge \nu$. By definition of j'_k and i'_k, it now follows that $j'_k \le k - 1$ for $1 \le k \le s$, and $i'_k \le k$ for $0 \le k \le s - 1$.

Now that we know that $p^{I'+J'} G(0, s - 1; I', G(1, s; J' + 1)$ is in fact a summand on the right-hand side of congruence (6.5), we prove the following proposition. Remark that obviously, we have $p^{I+J} = p^{I'+J'}$.

Proposition 9.1 *Let I, J, I' and J' be defined as above. Then,*

$$G(0, s, I)\, G(1, s - 1; J + 1) = G(0, s - 1; I')\, G(1, s; J' + 1).$$

Thus, we can identify each summand on the left-hand side of (6.5) with a summand on the right-hand side.

Proof By a direct computation, we have

$$
\begin{aligned}
&G(0,s;I)\,G(1,s-1;J+1)\\
&\quad= G(0,\nu-1;I)\,G(\nu,s;I)\,G(1,\nu-1;J+1)\,G(\nu,s-1;J+1) \text{ (by Lemma 8.4)}\\
&\quad= G(0,\nu-1;I)\,G(\nu,s;I+1)\,G(1,\nu-1;J+1)\,G(\nu,s-1;J) \text{ (by (9.1))}\\
&\quad= G(0,\nu-1;I)\,G(\nu,s-1;J)\,G(1,\nu-1;J+1)\,G(\nu,s;I+1) \text{ (commutation)}\\
&\quad= G(0,\nu-1;I')G(\nu,s-1;I')G(1,\nu-1;J'+1)G(\nu,s;J'+1) \text{ (by definition of } I', J')\\
&\quad= G(0,s-1;I')\,G(1,s;J'+1) \text{ (by Lemma 8.4)},
\end{aligned}
$$

so the statement follows. Note that the last equality follows since by definition of I' and J', $i'_\nu = j'_\nu = 0$, $k - i'_k \geq \nu$ and $k - j'_k \geq \nu$ for $k > \nu$. Thus, $G(0, s-1; I')$ and $G(1, s; J'+1)$ both split at ν. □

Since by Proposition 9.1, we can identify every summand on the left-hand side of Eq. (6.5) satisfying $I + J \leq s - 1$ with a summand on the right-hand side, both sides are equal modulo p^s and the proof of Theorem 4.3 is complete.

Remark The above arguments to prove the congruence $D3$ can be slightly simplified, as was shown to us by A. Mellit.

10 The examples of Batyrev and Kreuzer

In their paper Batyrev and Kreuzer [5] list several Laurent polynomials f with reflexive Newton polyhedron $\Delta(f)$, whose fibres are supposed to compactify to Calabi–Yau 3-folds with $h^{12} = 1$.

Example No. 24 in their list is

$$
\begin{aligned}
f := {}& 1/X_4 + X_2 + 1/X_1X_4 + 1/X_1X_3X_4 + 1/X_1X_2X_3X_4 + 1/X_3\\
&+ X_1/X_3 + X_2/X_3X_4 + X_1/X_3X_4 + X_1X_2/X_3X_4 + X_2/X_4\\
&+ 1/X_2X_4 + 1/X_1X_2X_4 + 1/X_1X_2 + 1/X_1 + 1/X_2X_3X_4\\
&+ X_4 + 1/X_2 + X_1 + X_1/X_4 + 1/X_3X_4 + X_3 + 1/X_2X_3.
\end{aligned}
$$

to which our Theorem 4.3 applies: the coefficients $a(n) := [f^n]_0$, where

$a(0) = 1, a(1) = 0, a(2) = 18, a(3) = 168, a(4) = 2430, a(5) = 37200, a(6) = 605340,$

satisfy the congruence $D3$ modulo p^s for arbitrary s.

The power series $\Phi(t) = \sum_{n=0}^{\infty} a(n)t^n$ is solution to a rather complicated fourth order linear differential equation $PF = 0$, where

$$
\begin{aligned}
P := {}& 97^2\theta^4 + 97t\theta(-291 - 1300\theta - 2018\theta^2 + 1727\theta^3)\\
&+ \cdots + 2^6 3^3 13^4 7457 \cdot t^{11}(\theta+1)(\theta+2)(\theta+3)(\theta+4)),
\end{aligned}
$$

(with $\theta := t\partial/\partial t$). This operator was determined by Metelitsyn [9].

Example Of particular interest is the much simpler Laurent polynomial f corresponding to No. 62 from the list of Batyrev and Kreuzer [5], which is given by

$$f := X_1 + X_2 + X_3 + X_4 + \frac{1}{X_1X_2} + \frac{1}{X_1X_3} + \frac{1}{X_1X_4} + \frac{1}{X_1^2X_2X_3X_4}.$$

Then, the coefficients $a(n)$ are given by $a(n) = 0$ if $n \neq 0 \mod 3$ and

$$a(3n) = \frac{(3n)!}{n!^3} \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}.$$

The Newton polyhedron $\Delta(f)$ is reflexive (see [5]), and hence by Theorem 4.3, the coefficients $a(n)$ satisfy the congruence (4.1) modulo p^s for arbitrary s. The power series $\Phi(t) = \sum_{n=0}^{\infty} a(3n)t^n$ is solution to a fourth order linear differential equation $PF = 0$, where the differential operator P is of Calabi–Yau type and is given by

$$P := \theta^4 - 3t(3\theta+2)(3\theta+1)(11\theta^2+11\theta+3) - 9t^2(3\theta+5)(3\theta+2)(3\theta+4)(3\theta+1).$$

Since in this example (as in many others), only the coefficients $a(n)$ with $n = 3k$ are nonzero, it would be good to prove the following congruence for this example:

$$\begin{aligned} &a(3(n_0 + n_1 p + \cdots + n_s p^s))a(3(n_1 + \ldots + n_{s-1} p^{s-2})) \\ &\quad \equiv a(3(n_0 + \cdots + n_{s-1} p^{s-1}))a(3(n_1 + \cdots + n_s p^{s-1})) \mod p^s. \end{aligned}$$

11 Behaviour under covering

The last example raises the question after a congruence among the k-fold coefficients if $a(n) \neq 0$ implies $k|n$. As before, we consider a Laurent polynomial f corresponding to Newton polyhedron $\Delta(f)$ with a unique interior point. Let $\mathcal{A}$ be the exponent matrix corresponding to f, and consider the vectors with integral entries in the kernel of $\mathcal{A}$. If there exists a positive integer k such that

$$\ell := \begin{pmatrix} \ell_1 \\ \vdots \\ \ell_m \end{pmatrix} \in \ker(\mathcal{A}) \Rightarrow k|(\ell_1 + \cdots + \ell_m),$$

then it follows that

$$a(n) := [f^n]_0 \neq 0 \Rightarrow k|n,$$

since for $l \in \mathbb{N}$,

$$[f^l]_0 = \sum_{(\ell_1,\ldots,\ell_m)\in A_{f,l}} \binom{l}{\ell_1, \ell_2, \ldots, \ell_m},$$

where

$$A_{f,l} := \ker(\mathcal{A}) \cap \{(\ell_1, \ldots, \ell_m) \in \mathbb{N}_0^m : \ell_1 + \cdots + \ell_m = l\}.$$

We are interested in the congruences

$$\begin{aligned} &a(k(n_0 + \cdots + n_s p^s))a(k(n_1 + \cdots + n_{s-1} p^{s-2})) \\ &\quad \equiv a(k(n_0 + \cdots + n_{s-1} p^{s-1}))a(k(n_1 + \cdots + n_s p^{s-1})) \mod p^s, \end{aligned} \tag{11.1}$$

which we will prove in general for $s = 1$, and which we will prove for one example by proving that the following condition is satisfied:

Condition 1 *For a tuple* $(\ell_1, \ldots, \ell_m)$ *with*

$$\ell_1 + \cdots + \ell_m = k\mu \le k(p-1),$$

it follows that

$$p \,\Bigg|\, \gcd\left(\sum_{j=1}^{m} a_{i,1}\ell_1, \ldots, \sum_{j=1}^{m} a_{j,n}\ell_j\right) \Rightarrow \sum_{j=1}^{m} a_{i,1}\ell_j = \cdots = \sum_{j=1}^{m} a_{j,n}\ell_j = 0.$$

Note that the proof is similar for many other examples which we will not treat in here. First of all, before we come to the example, we give a general proof of (11.1) for $s = 1$.

Proposition 11.1 *Let* $a(n), n \in \mathbb{N}$ *be an integral sequence satisfying*

$$a(n_0 + n_1 p) \equiv a(n_0)a(n_1) \mod p$$

for $0 \le n_0 \le p-1$ *and* $a(n) \ne 0$ *iff* $k|n$. *Then*

$$a(k(n_0 + n_1 p)) \equiv a(kn_0)a(kn_1) \mod p.$$

Proof If $kn_0 < p$, then the proposition follows directly. Hence let us assume that $kn_0 = n_0' + n_0'' p > p - 1$. Then

$$a(k(n_0 + n_1 p)) = a(n_0' + (kn_1 + n_0'')p) \equiv a(n_0')a(kn_1 + n_0'') \mod p.$$

Since $k \nmid nn_0'$ and $a(n_0') = 0$ by assumption, it follows on the one hand that

$$a(k(n_0 + n_1 p)) \equiv 0 \mod p.$$

On the other hand,

$$a(kn_0) = a(n_0' + n_0'' p) \equiv a(n_0')a(n_0'') \mod p \quad \text{where } a(n_0') = 0,$$

and thus $a(kn_0) \equiv 0 \mod p$ and

$$a(kn_0)\,, a(kn_1) \equiv 0 \mod p$$

so the proposition follows. □

11.1 An example

In the example of the Laurent polynomial No. 62 in the list of Batyrev and Kreuzer [5], the exponent matrix is

$$\mathcal{A} := \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & -1 & -1 & -2 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \end{pmatrix}.$$

A basis of $\ker(\mathcal{A})$ is given by

$$\left\{ \begin{pmatrix} 1\\1\\0\\0\\1\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\1\\0\\0\\1\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\0\\1\\0\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 2\\1\\1\\1\\0\\0\\0\\1 \end{pmatrix} \right\},$$

and thus it follows that $[f^n]_0 \neq 0 \Rightarrow 3|n$ and $k = 3$. We prove that Condition 1 is satisfied in this example. Assume that $p \neq 3$ and that

$$p \,\left|\, \gcd\left(\sum_{j=1}^{8} a_{1,j}\ell_j, \ldots, \sum_{j=1}^{8} a_{4,j}\ell_j\right)\right. \quad \text{for } \ell_1 + \cdots + \ell_8 = 3\mu \leq 3(p-1).$$

This means that there exist $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ such that

$$\begin{cases} \ell_1 = \ell_5 + \ell_6 + \ell_7 + 2\ell_8 + x_1 p \\ \ell_2 = \ell_5 + \ell_8 + x_2 p \\ \ell_3 = \ell_6 + \ell_8 + x_3 p \\ \ell_4 = \ell_7 + \ell_8 + x_4 p, \end{cases}$$

which implies

$$3(\ell_5 + \ell_6 + \ell_7 + 2\ell_8) + (x_1 + x_2 + x_3 + x_4)p = 3\mu \leq 3(p-1).$$

Thus, it follows that $(x_1 + \cdots + x_4) = 3z$ for some $z \in \mathbb{Z}$ and that

$$\ell_5 + \ell_6 + \ell_7 + 2\ell_8 + zp = \mu \leq p - 1.$$

Since $\ell_5, \ldots, \ell_8$ are nonnegative integers, it follows directly that $z \leq 0$. Now, consider the two following cases:

(1) Let $z = 0$. Then,

$$\ell_5 + \ell_6 + \ell_7 + 2\ell_8 \leq p - 1. \tag{11.2}$$

Assume that $x_i < 0$, i.e., $x_i \leq -1$ for some $1 \leq i \leq 4$. Since $\ell_1, \ldots, \ell_4$ are nonnegative integers, it follows that either $\ell_5 + \ell_6 + \ell_7 + 2\ell_8 \geq p$ or $\ell_j + \ell_8 \geq p$ for some $5 \leq j \leq 7$, a contradiction to (11.2). Thus, since $x_1 + x_2 + x_3 + x_4 = 0$, it follows that $x_1 = x_2 = x_3 = x_4 = 0$ and that

$$\sum_{j=1}^{8} a_{1,j}\ell_j = \cdots = \sum_{j=1}^{8} a_{4,j}\ell_j = 0$$

in this example.

(2) Let $z < 0$. Assume that $\ell_5 + \ell_6 + \ell_7 + 2\ell_8 < (-z+1)p$. Since $\ell_1 \geq 0$, it follows that $x_1 > z - 1$, and since x_1 is integral, that $x_1 \geq z$. Since $x_1 + x_2 + x_3 + x_4 = 3z$, it follows that $x_2 + x_3 + x_4 \leq 2z$. Now assume that $x_i \geq z$ for $2 \leq i \leq 4$. Then $x_2 + x_3 + x_4 \geq 3z$, a contradiction. Hence there exists an index i such that $x_i < z$, and hence $x_i \leq z - 1$. Since $\ell_i \geq 0$, it follows that $\ell_{i+2} + \ell_8 \geq (-z+1)p$, a contradiction since

$$\ell_{i+2} + \ell_8 \leq \ell_5 + \ell_6 + \ell_7 + 2\ell_8 < (-z+1)p$$

by assumption. Thus, we have $\ell_5 + \ell_6 + \ell_7 + 2\ell_8 \geq (-z+1)p$, which implies $p \leq \ell_5 + \ell_6 + \ell_7 + 2\ell_8 + zp \leq p - 1$, a contradiction.

Thus, it follows that the only possible case is $z = 0$, and $x_1 = x_2 = x_3 = x_4 = 0$, which proves that Condition 1 is satisfied in this example.

12 The statement D1

For the proof of congruence (4.1), the coefficients $c_{\mathbf{a}}$ of

$$f(X) = \sum_{\mathbf{a}} c_{\mathbf{a}} X^{\mathbf{a}}$$

did not play a role. This is different if one is interested in the proof of part D1 of the Dwork congruences. Let $n \in \mathbb{N}$, and write $n = n_0 + pn_1$, where $n_0 \leq p-1$. Then, to prove D1 for the sequence $a(n) := [f^n]_0$ means that one has to prove that

$$\frac{\left[f^{n_0+n_1 p}\right]_0}{[f^{n_1}]_0} \in \mathbb{Z}_p. \tag{12.1}$$

Sticking to the notation of the previous sections, we write

$$f^{n_0+n_1 p}(X) = f^{n_0}(X) f^{n_1}(X^p) + p f^{n_0}(X) g_{n-1,1}(X). \tag{12.2}$$

Assume that $p^k | [f^{n_1}]_0$. To prove (12.1), one has to prove that $p^k | [f^{n_0+n_1 p}]_0$. By (12.2), this is equivalent to proving that $p^{k-1} | [f^{n_0} g_{n_1,1}(X)]_0$. Thus, the proof of part D1 of the Dwork congruences requires an investigation in the p-adic orders of the constant terms of f^{n_1} and $g_{n_1,1}$ for arbitrary n_1, and requires methods that are completely different from the methods we applied to prove the congruence $D3$.

Acknowledgments We thank A. Mellit for his comments. The work of the first author was funded by the SFB Transregio 45 Mainz–Bonn–Essen.

References

1. Almkvist, G., van Enckevort, C., van Straten, D., Zudilin, W.: Tables of Calabi–Yau equations. arXiv:math/0507430
2. Apéry, R.: Irrationalité de $\zeta(2)$ et $\zeta(3)$. Asérisque **61**, 11–13 (1979)
3. Beukers, F.: Some congruences for the Apéry numbers. J. Number Theory **21**, 141–155 (1985)
4. Beukers, F.: Another congruence for the Apéry numbers. J. Number Theory **25**, 201–210 (1987)
5. Batyrev, V., Kreuzer, M.: Constructing new Calabi–Yau 3-folds and their mirrors via conifold transitions. Adv. Theor. Math. Phys. **14**(3), 879–898 (2010)
6. Doran, C., Kerr, M.: Algebraic K-theory of toric hypersurfaces. CNTP **5**(2), 397–600 (2011)
7. Duistermaat, J., van der Kallen, W.: Constant terms in powers of a Laurent polynomial. Indag. Math. **9**, 221–231 (1998)
8. Dwork, B.: p-adic cycles. Publ. Math. de l'I.H.E.S., tome **37**, 27–115 (1969)
9. Metelitsyn, P.: How to compute the constant term of a power of a Laurent polynomial efficiently. arXiv:1211.3959
10. Samol, K., van Straten, D.: Frobenius polynomials for Calabi–Yau equations. Commun. Number Theory Phys. **2**(3), 537–561 (2008)
11. Jeng-Daw, Yu.: Notes on Calabi–Yau ordinary differential equations. Commun. Number Theory Phys. **3**(3), 475–493 (2009)