DWORK CONGRUENCES AND REFLEXIVE POLYTOPES

KIRA SAMOL AND DUCO VAN STRATEN

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.

1. Dwork congruences

Definition 1.1. *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

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

D2

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

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

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

we find by repeated application that

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

In fact, this is easily seen to be equivalent to $D3$ for $s = 0$.
Similarly, for higher s the congruences $D3$ are equivalent to

$$a(n_0 + \ldots + n_{s+1}p^{s+1})a(n_1 + \ldots + n_s p^{s-1}) \equiv$$

$$a(n_0 + \ldots + n_s p^s)a(n_1 + \ldots + n_{s+1}p^s) \mod p^{s+1}. \tag{1.1}$$

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

$$n \mapsto a(n)/a(\lfloor n/p\rfloor)$$

This work is entirely supported by DFG Sonderforschungsbereich/Transregio 45.

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 [Dw], Theorem 3.)

Theorem 1.2. *Let $(a(n))_n$ be a $\mathbb{Z}_p$−valued sequence satisfying the Dwork congruences* D1 *and* D2 *. Let*

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

and

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

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

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

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

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

The congruences were used in [SvS] to determine Frobenius polynomials associated to Calabi-Yau motives coming from fourth order operators of Calabi-Yau type from the list [AESZ]. 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 [Yu]. 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.

2. Laurent polynomials

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

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

to write a general Laurent-polynomial as

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

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

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

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

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

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;

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

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 2.1. *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*

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

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

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

We have

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

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

$$v := \frac{\ell_1}{g}\mathbf{a_1} + ... + \frac{\ell_m}{g}\mathbf{a}_m \in \mathbb{Z}^n$$

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

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

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.*

3. The fundamental period

Notation 3.1. *For a Laurent-polynomial we denote by* $[f]_0$ *the* constant term*, that is, the coefficient of the monomial* X^0.

Definition 3.2. *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

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

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

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

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

Theorem 3.3. *Let* $f \in \mathbb{Z}[X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}]$ *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*

$$a(n_0 + ... + n_s p^s)a(n_1 + ... + n_{s-1}p^{s-2}) \equiv$$

$$a(n_0 + ... + n_{s-1}p^{s-1})a(n_1 + ... + n_s p^{s-1}) \mod p^s. \tag{3.1}$$

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

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.

4. Proof for the congruence mod p

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

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

The proof we will give is completely elementary; the key ingredient is theorem 2.1, which states that for all non-negative integral $\ell = (\ell_1, ..., \ell_m)$ one has,

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

Proposition 4.1. *Let f be a Laurent polynomial as above and $n_0 < p$. Then*

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

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

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

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 $X_1^p, ..., X_n^p$, since all monomials in $f^{n_1}(X^p)$ are monomials in $X_1^p, ..., X_n^p$.
A monomial

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

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

$$n_0 = \ell_1 + ... + \ell_m$$

of n_0 in non-negative integers ℓ_i. If M were a monomial in $X_1^p, ..., X_n^p$, then we would have the divisibility

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

and hence

$$p \mid \gcd_{i=1,...,n} (\sum_{j=1}^{m} a_{i,j}\ell_j).$$

On the other hand, by 2.1 we have

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

So we conclude that $\sum_{i=1}^{m} a_{i,j}\ell_j = 0$ for $1 \le j \le n$ and that the monomial M is the constant monomial X^0. Hence it follows that

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

and since

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

the proposition follows. □

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

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

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

5. Strategy for higher s

The idea for the higher congruences is basically the *same as for* $s = 1$, but is combinatorically more involved. Surprisingly, one does not need any statements stronger than 2.1. To prove the congruence 3.1, we have to show that

$$\left[\prod_{k=0}^{s} f^{n_k p^k}\right]_0 \left[\prod_{k=1}^{s-1} f^{n_k p^{k-1}}\right]_0 \equiv \left[\prod_{k=0}^{s-1} f^{n_k p^k}\right]_0 \left[\prod_{k=1}^{s} f^{n_k p^{k-1}}\right]_0 \mod p^s. \tag{5.1}$$

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

Proposition 5.1. *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

$$p^k g_{n,k}(X) := f(X)^{np^k} - \sum_{j=0}^{k-1} p^j g_{n,j}(X^{p^{k-1-j}}). \tag{5.2}$$

Proof. We have to prove that the right-hand side of equation 5.2 is divisible by p^k. This is proved by induction on k and an application of the congruence

$$f(X)^{p^m} \equiv f(X^p)^{p^{m-1}} \mod p^m. \tag{5.3}$$

For $k = 1$, the divisibility follows directly by (5.3). Assume that the statement is true for $m \leq k-1$. 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 $f(X)^{np^k} - \sum_{j=0}^{k-1} p^j g_{n,j}(X^{p^{k-j}}) \equiv 0 \mod p^n$. □

The congruences involve constant term expressions of the form

$$\begin{aligned} \left[\prod_{k=a}^{b} f^{n_k p^k}\right]_0 &= \left[\prod_{k=a}^{b} \sum_{j=0}^{k} p^j g_{n_k,j}(X^{p^{k-j}})\right]_0 \\ &= \sum_{i_a \leq a} \dots \sum_{i_b \leq b} p^{\sum_{k=a}^{b} i_k} \left[\prod_{k=a}^{b} g_{n_k,i_k}(X^{p^{k-i_k}})\right]_0 . \end{aligned} \tag{5.4}$$

Thus, equation (5.1) translates into

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

(5.5) mod p^s

Since this congruence is supposed to hold modulo p^s, on the left-hand side, only the summands 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 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 equation 5.1. 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.

6. Splitting positions

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

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

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

Definition 6.1. *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 $G(a,\ell-1;I)$ we mean the expression corresponding to the sequence $(i_a, ..., i_{\ell-1})$, while by $G(\ell,b;I)$, we mean the expression corresponding to $(i_\ell, ..., i_b)$. Note that $\ell = a$ represents a trivial splitting, but splitting at $\ell = b$ is a non-trivial property.

Proposition 6.2. *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

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

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

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

It follows from the assumptions that the product $G(\ell,b;I) = \prod_{k=\ell}^{b} g_{n_k,i_k}(X^{p^{k-i_k}})$ 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

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

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

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

so that

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

It follows that

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

Hence, it follows that

$$p^\ell \mid \gcd_{i=1,...,n}(\sum_{j=1}^{m} a_{i,j}\gamma_j) \leq \sum_{j=1}^{m}\gamma_j < p^\ell,$$

where the first inequality follows from Theorem 2.1. This implies $\sum_{j=1}^{m} a_{i,j}\gamma_j = 0$ for $1 \le i \le n$. But this means that the monomial in $\prod_{k=t}^{s-1} g_{n_k,i_k}(X^{p^{k-i_k}})$ is itself constant. $\square$

Now that we know that we can split up expressions $G(a,b;I)$ satisfying the condition given in Proposition 6.2, we proceed by proving that all the summands on both sides of equation 5.5 that do not have a coefficient divisible by p^s satisfy this splitting condition.

7. Three combinatorical Lemmas

In this section, we prove three simple combinatorical lemmas which will be applied to split up expressions $G(0,s;I)G(1,s-1;J+1)$ that occur in the congruence (5.1).

Definition 7.1. *Let $a \le b$ and $I = (i_a, i_{a+1}, \dots, i_b)$ 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 6.2 and that $i_\ell = 0$.

Lemma 7.2. *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 $\mathcal{N} := \{k \ | i_k = 0\}$ 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 $k_1 < ... < k_m$, it follows that $i_\nu \ge m+1$.
Now assume that we have μ different violating indices $\nu_1, ..., \nu_\mu$ and that ν_j is a violating index for all $j \in \mathcal{N}_j$, where we partition $\mathcal{N}$ into disjoint subsets

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

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. $\square$

We can sharpen lemma 7.2 to:

Lemma 7.3. *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 7.2. 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 $\{i_a, ..., i_b\} = \{i_a, ..., i_{\nu-1}\} \cup \{i_\nu, ..., i_b\}$ in position ν such that $\sum_{k=a}^{\nu-1} i_k = N_\nu$ and $\sum_{k=\nu}^{b} i_k = b - a - m - 1 - N_\nu$. Depending on N_ν, we have to distinguish between the following cases:

(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 $(i_\nu, ..., i_b)$, and thus for the whole $(i_a, ..., i_b)$, there exist at least $m + 1$ such indices.
(2) The case $N_\nu \leq (\nu - 1) - a - 1$ splits up in two cases:
   (a) $N_\nu \leq (\nu - 1) - a - m$. By induction, $(i_a, ..., i_{\nu-1})$ has at least m splitting indices, and the whole $(i_a, ..., i_b)$ has at least $m + 1$ such indices.
   (b) $N_\nu = (\nu-1)-a-n$, where $1 \leq n \leq m$. Since $\sum_{k=a}^{\nu-1} i_k = (\nu-1)-a-n$, by induction for $(i_a, ..., i_{\nu-1})$ exist at least n splitting indices. Since $\sum_{k=\nu}^{b} i_k = b - \nu - (m - n)$, for $(i_\nu, ..., i_b)$, there exist at least $m - n$ splitting indices. Thus, for the whole $(i_a, ..., i_b)$ exist at least $n+(m-n)+1 = m+1$ splitting indices.

□

Lemma 7.4. (1) *Let $I = (i_0, ..., i_s)$ and $J = (j_1, ..., j_{s-1})$ 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,

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

(2) *Let $I = \{i_0, ..., i_{s-1}\}$ and $J = (j_1, ..., j_s)$ 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. (1) Note that since $S_I \cup S_J \cup \{1, s\} \subset \{1, 2, ..., s\}$, 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 7.3. 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 7.3. 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.
(2) Note that since $(S_I \cup \{s\}) \cup (S_J \cup \{1\}) \subset \{1, ..., s\}$, 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 $\sum_{k=1}^{s} j_k \leq s - 1 - (s - \#S_I - 1)$, and $\#S_J \geq s - \#S_I - 1$. 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.

□

8. Proof for higher s

We will use the combinatorical lemmas on splitting indices from the last section to prove the congruence (5.1) modulo p^s.
For a sequence $I = (i_a, ..., i_b)$, we write

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

For a sequence $J = (j_a, ..., j_b)$, we define $J + 1 := (j_a + 1, ..., j_b + 1)$.
Note that if $k - j_k > 0$ for $a \leq k \leq b$, then we have

$$G(a, b; J + 1) = G(a, b; J), \tag{8.1}$$

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 (5.5) defined by the tuple (I, J) with $\sum_{k=0}^{s} i_k + \sum_{k=1}^{s-1} j_k \leq s - 1$, and let $1 \leq \nu \leq s$ be such that $G(0, s; I)$ splits in position ν and either $G(1, s - 1; J + 1)$ splits in position ν or $\nu \in \{1, s\}$. Such a ν exists by Lemma (7.4). Define $I' = (i'_0, ..., i'_{s-1})$ and $J' = (j'_1, ..., j'_s)$ by

$$\begin{aligned} i'_k &= i_k \text{ for } k \leq \nu - 1 \\ i'_k &= j_k \text{ for } k \geq \nu \\ j'_k &= j_k \text{ for } k \leq \nu - 1 \\ j'_k &= i_k \text{ for } k \geq \nu. \end{aligned}$$

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 (5.5), we have to explain why $i'_k \leq k$ and $j'_k \leq k - 1$. Note that $j_k \leq k - 1$ for $1 \leq k \leq s - 1$ and $i_k \leq k$ for $0 \leq k \leq s$. Furthermore, we have $i_k \leq k - 1$ for $k \geq \nu$ since $i_\nu = 0$ and $G(0, s; I)$ splits in position ν, which means that $k - i_k \geq \nu \geq 1$ for $k \geq \nu$.
By definition of j'_k and i'_k, it now follows that $j'_k \leq k - 1$ for $1 \leq k \leq s$, and $i'_k \leq k$ for $0 \leq k \leq s - 1$.
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 (5.5), we prove the following Proposition. Remark that obviously, we have $p^{I+J} = p^{I'+J'}$.

Proposition 8.1. *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 (5.5) with a summand on the right-hand side.

Proof. By a direct computation:

$$\begin{aligned} & G(0, s; I)G(1, s - 1; J + 1) \\ = \;& G(0, \nu - 1; I)G(\nu, s; I)G(1, \nu - 1; J + 1)G(\nu, s - 1; J + 1) \text{ by lemma 7.4} \\ = \;& G(0, \nu - 1; I)G(\nu, s; I + 1)G(1, \nu - 1; J + 1)G(\nu, s - 1; J) \text{ by (8.1)} \\ = \;& G(0, \nu - 1; I)G(\nu, s - 1; J)G(1, \nu - 1; J + 1)G(\nu, s; I + 1) \text{ (commutation)} \\ = \;& G(0, \nu - 1; I')G(\nu, s - 1; I')G(1, \nu - 1; J' + 1)G(\nu, s; J' + 1) \text{ by definition of } I',\ J' \\ = \;& G(0, s - 1; I')G(1, s; J' + 1) \text{ by lemma 7.4,} \end{aligned}$$

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 8.1, we can identify every summand on the left-hand side of equation (5.5) 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 3.3 is complete.

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

9. An Example

Let f be the Laurent-polynomial

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

It is No. 24 in the list of Batyrev and Kreuzer [BK], so $\Delta(f)$ is a reflexive polytope and our theorem 3.3 applies: the coefficients $a(n) := [f^n]_0$

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

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 fourth order linear differential equation $PF = 0$, where the differential operator P is of Calabi-Yau type

$$\begin{aligned} P &:= 885010054\theta^4 + t(9123382\theta(-291 - 1300\theta - 2018\theta^2 + 1727\theta^3) + ... \\ &+ t^{11}(3461674786667136(\theta+1)(\theta+2)(\theta+3)(\theta+4)), \end{aligned}$$

(where $\theta := t\partial/\partial t$) that was determined in [PM].

10. Behaviour under Covering

Let f be a Laurent-polynomial corresponding to a reflexive polyhedron, 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

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

then it follows that

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

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

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

where

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

We are interested in the congruences

$$\begin{aligned} &a(k(n_0 + ... + n_s p^s))a(k(n_1 + ... + n_{s-1}p^{s-2})) \equiv \\ (10.1) \qquad &a(k(n_0 + ... + n_{s-1}p^{s-1}))a(k(n_1 + ... + n_s p^{s-1})) \mod p^s, \end{aligned}$$

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 $(\ell_1, ..., \ell_m)$ with*

$$\ell_1 + ... + \ell_m = k\mu \leq k(p-1),$$

it follows that

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

Note that the proof is simliar 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 (10.1) for $s = 1$.

Proposition 10.1. *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 $0 \leq n_0 \leq p-1$ and $a(n) \neq 0$ 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 assume that $kn_0 = n_0' + n_0'' p > p - 1$. Then

$$\begin{aligned} a(k(n_0 + n_1 p)) &= a(n_0' + (kn_1 + n_0'')p) \\ &\equiv a(n_0')a(kn_1 + n_0'') \mod p. \end{aligned}$$

Since $k \not| n_0'$ and $a(n_0') = 0$ by assumption, it follows that

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

On the other hand, $a(kn_0) = a(n_0' + n_0'' p) \equiv a(n_0')a(n_0'') \mod p$ where $a(n_0') = 0$, and thus $a(kn_0) \equiv 0 \mod p$ and

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

and the proposition follows. □

10.1. **An Example.** Let f be the Laurent-polynomial No. 62 in the list of Batyrev and Kreuzer [BK], which is given by

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

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 [BK]), and hence by Theorem 3.3, the coefficients $a(n)$ satisfy the congruence $D3$ 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

$$\begin{aligned} P &:= \theta^4 - 3t(3\theta+2)(3\theta+1)(11\theta^2+11\theta+3) \\ &- 9t^2(3\theta+5)(3\theta+2)(3\theta+4)(3\theta+1). \end{aligned}$$

In this example, 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

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

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

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

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

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

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 $(x_1 + ... + x_4) = 3z$ for some $z \in \mathbb{Z}$ and that

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

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

(1) $z = 0$: Then,

$$\ell_5 + \ell_6 + \ell_7 + 2\ell_8 \leq p - 1 \tag{10.2}$$

Assume that $x_i < 0$, i.e. $x_i \leq -1$ for some $1 \leq i \leq 4$. Since $\ell_1, ..., \ell_4$ 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 (10.2). 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

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

in this example.

(2) $z < 0$: 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.

11. The statement D1

For the proof of congruence (3.1), 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

$$\frac{[f^{n_0+n_1p}]_0}{[f^{n_1}]_0} \in \mathbb{Z}_p. \tag{11.1}$$

Sticking to the notation of the previous sections, we write

$$f^{n_0+n_1p}(X) = f^{n_0}(X)f^{n_1}(X^p) + pf^{n_0}(X)g_{n-1,1}(X). \tag{11.2}$$

Assume that $p^k | [f^{n_1}]_0$. To prove (11.1), one has to prove that $p^k | [f^{n_0+n_1p}]_0$. By (11.2), 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 $D3$.

Acknowledgement. We thank A. Mellit for his comments. The work of the first author was funded by the SFB Transregio 45.

References

[AESZ] G. Almkvist, C. van Enckevort, D. van Straten, W. Zudilin, *Tables of Calabi-Yau Equations*, `arXiv:math/0507430`.

[BK] Batyrev, Kreuzer, *Constructing new Calabi-Yau 3-folds and their mirrors via conifold transitions* `arXiv:0802.3376v2`

[DK] C. Doran, M. Kerr, *Algebraic K-theory of toric hypersurfaces*, `ArXiv 0809.4669v1`.

[DvK] J. Duistermaat, W. van der Kallen, *Constant terms in powers of a Laurent polynomial*, Indagationes Math. **9**, (1998), 221-231.

[Dw] B. Dwork, *p-adic cycles*, Publications mathématiques de l'I.H.E.S., tome 37, 1969, 27-115.

[PM] P. Metelytsin, in preparation.

[SvS] K. Samol, D. van Straten, *Frobenius Polynomials for Calabi-Yau equations*, Communications in Number Theory and Physics, vol 2, no 3, (2008)

[Yu] Jeng-Daw Yu, *Notes on Calabi-Yau ordinary differential equations* `arXiv:0810.4040v1`