DWORK'S CONGRUENCES FOR THE CONSTANT TERMS OF POWERS OF A LAURENT POLYNOMIAL

ANTON MELLIT, MASHA VLASENKO

Abstract. We prove that the constant terms of powers of a Laurent polynomial satisfy certain congruences modulo prime powers. As a corollary, the generating series of these numbers considered as a function of a p-adic variable satisfies a non-trivial analytic continuation property, similar to what B. Dwork showed for a class of hypergeometric series.

1. Congruences

We shall prove the following

Theorem 1. *Let $\Lambda(x) \in \mathbb{Z}_p[x_1^{\pm 1}, \dots, x_d^{\pm 1}]$ be a Laurent polynomial, and consider the sequence of the constant terms of powers of Λ*

$$b_n \;=\; \Big[\Lambda(x)^n\Big]_0, \quad n = 0, 1, 2, \dots$$

Define

$$f(X) \;=\; \sum_{n=0}^{\infty} b_n X^n$$

and

$$f_s(X) \;=\; \sum_{n=0}^{p^s-1} b_n X^n\,, \quad s = 0, 1, 2, \dots$$

If the Newton polyhedron of Λ contains the origin as its only interior integral point, then for every $s \geq 1$ one has the congruence

$$\frac{f(X)}{f(X^p)} \;\equiv\; \frac{f_s(X)}{f_{s-1}(X^p)} \mod p^s \mathbb{Z}_p[[X]]\,, \tag{1}$$

or, equivalently, for every $s \geq 1$

$$f_{s+1}(X) f_{s-1}(X^p) \;\equiv\; f_s(X) f_s(X^p) \mod p^s \mathbb{Z}_p[X]\,. \tag{2}$$

One can easily see that congruence (1) with $s = 1$ is equivalent to the statement that for every n

$$b_n \;\equiv\; b_{n \bmod p}\, b_{\lfloor \frac{n}{p} \rfloor} \mod p\,,$$

or if we expand n to the base p as $n = n_0 + n_1 p + \dots + n_r p^r = \overline{n_0 \dots n_r}$ with digits $0 \leq n_i \leq p-1$ then

$$b_n \;\equiv\; b_{n_0} \dots b_{n_r} \mod p\,.$$

Date: June 26, 2013.

In [4] Duco van Straten and Kira Samol gave a generalization modulo higher powers of p: under the same assumptions as in Theorem 1 one has

$$b_{n+mp^s}\, b_{\lfloor \frac{n}{p} \rfloor} \equiv b_n\, b_{\lfloor \frac{n}{p} \rfloor + mp^{s-1}} \mod p^s \tag{3}$$

for all $n, m \geq 0$, $s \geq 1$. We do not know whether it is possible to deduce congruences (1)-(2) from (3). Our method of proof is independent and actually allows one to get (3) as a byproduct. In fact the main idea used here appeared as an attempt to give an independent proof of (3), and later we realized that it can also be applied to (1)-(2).

Throughout the paper we assume p to be a fixed prime number. For a natural number $n \in \mathbb{N}$ we denote by $\ell(n) = \lfloor \frac{\log n}{\log p} \rfloor + 1$ the length of the expansion of n to the base p, and we assume $\ell(0) = 1$. For any tuple of non-negative integers $n^{(1)}, \dots, n^{(r)}$ with $n^{(r)} \neq 0$ we introduce the notation

$$n^{(1)} * \cdots * n^{(r)} := n^{(1)} + n^{(2)} p^{\ell(n^{(1)})} + \cdots + n^{(r)} p^{\ell(n^{(1)}) + \cdots + \ell(n^{(r-1)})},$$

that is the expansion of $n^{(1)} * \cdots * n^{(r)}$ to the base p is the concatenation of the respective expansions of $n^{(1)}, \dots, n^{(r)}$.

The proof of Theorem 1 is based on the following

Lemma 1. *Under the assumptions of Theorem 1, there exists a $\mathbb{Z}_p$-valued sequence $\{c_n; n \geq 0\}$ such that for all $n \geq 1$*

$$b_n = \sum_{n^{(1)} * \cdots * n^{(r)} = n} c_{n^{(1)}} \cdot \ldots \cdot c_{n^{(r)}}, \tag{4}$$

where the sum runs over all $1 \leq r \leq \ell(n)$ and all possible partitions of the expansion of n to the base p into r expansions of non-negative integers, and

$$c_n \equiv 0 \mod p^{\ell(n)-1}. \tag{5}$$

The paper is organized as follows. We construct the sequence $\{c_n; n \geq 0\}$ in Sections 2-4. Section 5 can be read independently of the previous three, we deduce Theorem 1 from Lemma 1 in there.

In the remainder of this section we would like to suggest an application of the congruences stated in Theorem 1. Basically, we extract the following lemma from [1] (see Theorem 3). But since our setup is simpler and assumptions look slightly different, we give a proof nevertheless. Let us fix the following notation:

$|\cdot|_p$ denotes the p-adic norm, chosen so that $|p|_p = p^{-1}$

Ω = completion of the algebraic closure of $\mathbb{Q}_p$

$\mathcal{O}$ = ring of integers of $\Omega = \{z \in \Omega : |z|_p \leq 1\}$

$\mathcal{B}$ = ideal of non units in $\mathcal{O} = \{z \in \Omega : |z|_p < 1\}$

Lemma 2 (Dwork)**.** *Let a $\mathbb{Z}_p$-valued sequence $\{b_n; n \ge 0\}$ be such that b_0 is a unit and congruence* (1) *holds true for every $s \ge 1$. Consider the region*

$$\mathcal{D} \;=\; \left\{ z \in \mathcal{O} \;:\; |f_1(z)|_p \;=\; 1 \right\}.$$

Then

(i) *$\mathcal{D}$ contains $\mathcal{B}$, and if $z \in \mathcal{D}$ then $z^p \in \mathcal{D}$;*
(ii) *for every $s \ge 0$ one has $|f_s(z)|_p = 1$ when $z \in \mathcal{D}$;*
(iii) *the sequence of rational functions $f_s(z)/f_{s-1}(z^p)$ converges uniformly in $\mathcal{D}$, and if we denote the limiting analytic function by $\omega(z) = \lim\limits_{s\to\infty} f_s(z)/f_{s-1}(z^p)$ then for all $s \ge 1$*

$$\sup_{z\in\mathcal{D}} \Bigl| \omega(z) \;-\; \frac{f_s(z)}{f_{s-1}(z^p)} \Bigr|_p \;\le\; \frac{1}{p^s}\,;$$

(iv) *$f(z)/f(z^p)$, which is a power series with integral coefficients and hence an analytic function on $\mathcal{B}$, is the restriction of $\omega(z)$ to $\mathcal{B}$.*

Proof. As b_0 is a unit, for $z \in \mathcal{B}$ we have $|f_1(z)|_p = |b_0|_p = 1$ by the isosceles triangle principle for non-Archimedean norms. Since $f_1(X) \in \mathbb{Z}_p[X]$ then $f_1(X)^p - f_1(X^p) \in p\mathbb{Z}_p[X]$ and therefore $|f_1(z)^p - f_1(z^p)|_p \le \frac{1}{p}$ for any $z \in \mathcal{O}$. Hence for $z \in \mathcal{D}$ we have $|f_1(z^p)|_p = |f_1(z)^p| = 1$ again by the isosceles triangle principle, so $z^p \in \mathcal{D}$. (ii) follows from the same argument by induction on s, since for every $s \ge 1$ we have $f_s(X) - f_1(X)f_{s-1}(X^p) \in p\mathbb{Z}_p[X]$. To prove (iii) we notice that $f_k(X)f_{s-1}(X^p) - f_{k-1}(X^p)f_s(X) \in p^s\mathbb{Z}_p[X]$ for any $k \ge s$, which together with (ii) gives

$$\Bigl| \frac{f_k(z)}{f_{k-1}(z^p)} \;-\; \frac{f_s(z)}{f_{s-1}(z^p)} \Bigr|_p \le \frac{1}{p^s} \qquad \forall z \in \mathcal{D}\,,$$

and we see that this sequence of functions is a Cauchy sequence. To prove (iv) observe that

$$\Bigl| \frac{f(z)}{f(z^p)} \;-\; \frac{f_s(z)}{f_{s-1}(z^p)} \Bigr|_p \le \frac{1}{p^s}$$

for any $z \in \mathcal{B}$ as $f(X)/f(X^p) - f_s(X)/f_{s-1}(X^p) \in p^s\mathbb{Z}_p[[X]]$. □

Let us take for example the Laurent polynomial

$$\Lambda(x_1, x_2) \;=\; \frac{(1+x_1)(1+x_2)(1+x_1+x_2)}{x_1 x_2}\,.$$

One can show that the sequence of the constant terms of its powers is the Apéry sequence

$$b_n \;=\; \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}\,.$$

Conditions of Theorem 1 are satisfied for all primes p since coefficients are integral and the Newton polygon of Λ has one interior integral point. Normalizations of the smooth fibers of the family

$$E_t \;:\; \Lambda(x_1, x_2) \;=\; \frac{1}{t}$$

are elliptic curves. We denote by $\overline{E}_t \subset \mathbb{P}^2$ the normalization of E_t. Now fix any prime p and consider the above family over the finite field $\mathbb{F}_p$. Assume that $t \in \mathbb{F}_p^\times$ is such that $\overline{E}_t$ is smooth. Let $z_t \in \mathbb{Z}_p$ be the respective Teichmüller representative, that is the unique p-adic number satisfying $z_t^{p-1}=1$ and $z_t \equiv t \mod p$. One can show that

$$p+1-\#\overline{E}_t(\mathbb{F}_p) \equiv f_1(t) \mod p\,.$$

Hence $f_1(t)$ modulo p is the Hasse invariant for this family, and we have $|f_1(z_t)|_p=1$ precisely when the curve $\overline{E}_t$ is ordinary. The number $\omega(z_t)$ is then a reciprocal zero of the zeta function of $\overline{E}_t/\mathbb{F}_p$, i.e.

$$\mathcal{Z}\Big(\overline{E}_t/\mathbb{F}_p;X\Big) = \frac{(1-\omega(z_t)X)(1-\frac{p}{\omega(z_t)}X)}{(1-X)(1-pX)}\,.$$

The reciprocal zero which is a p-adic unit is usually called the "unit root", which allows to distinguish between the two reciprocal roots in the case of ordinary reduction. We plan to devote another paper to the proof of such "unit root formulas". Lemma 2 also shows that to get the first s p-adic digits of the unit root it is sufficient to compute $f_s(z_t)/f_{s-1}(z_t)$ modulo p^s.

This situation resembles the classical example with the Legendre family due to John Tate and Bernard Dwork (see §8 in [3], §5 in [2]). Theorem 1 along with Lemma 2 constitute a step towards proving such "unit root formulas" for families of hypersurfaces.

2. Ghost terms

For a Laurent polynomial $\Lambda(x)\in\mathbb{Z}_p[x_1^{\pm1},\dots,x_d^{\pm1}]$ and an integer $m\geq1$ we write $\Lambda(x^m)$ for $\Lambda(x_1^m,\dots,x_d^m)$. The Newton polyhedron of Λ is the convex hull in $\mathbb{R}^d$ of the exponent vectors of the monomials of Λ. It is denoted by $\mathrm{Newt}(\Lambda)$.

Definition. *For a Laurent polynomial $\Lambda(x)$ and an integer $s\geq1$ the ghost term $R_s(\Lambda)$ is the Laurent polynomial defined by*

$$R_s(\Lambda)(x) := \Lambda(x)^{p^s}-\Lambda(x^p)^{p^{s-1}}\,.$$

In addition we put $R_0(\Lambda):=\Lambda$.

Proposition 1. *For every integer $s\geq0$ one has*

(i) $\Lambda(x)^{p^s} = R_0(\Lambda)(x^{p^s})+R_1(\Lambda)(x^{p^{s-1}})+\dots+R_s(\Lambda)(x)$;
(ii) $R_s(\Lambda)\equiv 0 \mod p^s$;
(iii) $\mathrm{Newt}(R_s(\Lambda))\subset p^s\,\mathrm{Newt}(\Lambda)$.

Proof. Formula (i) easily follows by induction. (ii) is trivial when $s=0$ and clearly $p|\Lambda(x)^p-\Lambda(x^p)$ which proves the statement for $s=1$. To do induction in s we use the fact that in any ring R if $X\equiv Y \pmod{p^s}$ then $X^p\equiv Y^p \pmod{p^{s+1}}$. This proves (ii). (iii) follows from the definition of ghost terms and the following two obvious properties of the Newton polyhedron: for any Laurent polynomial Φ and any integer $m\geq1$ one has $\mathrm{Newt}(\Phi(x)^m)\subset m\ \mathrm{Newt}(\Phi(x))$ and $\Phi(x^m)\subset m\,\mathrm{Newt}(\Phi(x))$. □

Expanding any positive integer n to the base p as $n=n_0+n_1p+\dots+n_{\ell(n)-1}p^{\ell(n)-1}$ with digits $0\leq n_i\leq p-1$ we use (i) in the above proposition to decompose the product

$$\Lambda^n=\Lambda^{n_0}(\Lambda^{n_1})^p\dots(\Lambda^{n_{\ell(n)-1}})^{p^{\ell(n)-1}}$$

as the sum of products of ghost terms of the collection of p Laurent polynomials Λ^a, $0 \le a \le p-1$. We obtain that $\Lambda(x)^n$ is the sum of the products

$$R^n_{m,\Lambda}(x) := \prod_{i=0}^{\ell(n)-1} R_{m_i}(\Lambda^{n_i})(x^{p^{i-m_i}})$$

where $m = (m_0, m_1, \dots, m_{\ell(n)-1})$ runs over the set of all integral tuples of length $\ell(n)$ satisfying $0 \le m_i \le i$. For such a tuple we denote $|m| = \sum m_i$. Then one has

$$R^n_{m,\Lambda}(x) \;\equiv\; 0 \mod p^{|m|}$$

from (ii) in the above proposition, and (iii) gives us

$$\mathrm{Newt}\Big(R^n_{m,\Lambda}\Big) \subset n\;\mathrm{Newt}(\Lambda)$$

respectively.

3. Indecomposable tuples

Denote the set of all tuples $(m_0, m_1, \dots, m_{k-1}) \in \mathbb{Z}^k$ satisfying $0 \le m_i \le i$ by S_k. Put $S = \cup_{k>0} S_k$. For $m' \in S_k$, $m'' \in S_l$ we denote $m' * m'' = (m'_0, \dots, m'_{k-1}, m''_0, \dots, m''_{l-1}) \in S_{k+l}$.

Definition. *A tuple $m \in S$ is called indecomposable if it cannot be presented as $m' * m''$ for $m', m'' \in S$. The set of all indecomposable tuples of length k is denoted as S^{ind}_k and we put $S^{ind} = \cup_{k>0} S^{ind}_k$.*

Recall the notation $|m| = \sum m_i$ for a tuple $m \in S$. We have

Proposition 2. *If $m \in S^{ind}_k$, then $|m| \ge k-1$.*

Proof. If m is indecomposable then for each $i \in \{1, \dots, k-1\}$ there exists $j \ge i$ such that $m_j > j - i$, i.e. $j \ge i > j - m_j$. The number of such i for a given j is m_j. The total number of i is $k-1$, therefore the sum of m_j is at least $k-1$. □

For a Laurent polynomial Λ, integer $n \ge 1$ and tuple $m \in S_{\ell(n)}$ we defined in the previous section the product of ghost terms $R^n_{m,\Lambda}$, so that $\Lambda^n = \sum_{m \in S_{\ell(n)}} R^n_{m,\Lambda}$. Now we introduce Laurent polynomials

$$I^n_\Lambda := \sum_{m \in S^{ind}_{\ell(n)}} R^n_{m,\Lambda}\,.$$

We summarize their properties in the following

Proposition 3. *For every integer $n \ge 1$ one has*

(i) $\Lambda(x)^n = \sum_{n = n^{(1)} * \dots * n^{(r)}} I^{n^{(1)}}_\Lambda(x)\, I^{n^{(2)}}_\Lambda(x^{p^{\ell(n^{(1)})}}) \;\cdots\; I^{n^{(r)}}_\Lambda(x^{p^{\ell(n^{(1)})+\ell(n^{(2)})+\dots+\ell(n^{(r-1)})}})$
where the sum runs over all $1 \le r \le \ell(n)$ and all possible partitions of the expansion of n to the base p into r expansions of non-negative integers;

(ii) $I^n_\Lambda \;\equiv\; 0 \mod p^{\ell(n)-1}$;

(iii) $\mathrm{Newt}(I^n_\Lambda) \subset n\,\mathrm{Newt}(\Lambda)$.

Proof. We start with the formula $\Lambda^n = \sum_{m \in S_{\ell(n)}} R^n_{m,\Lambda}$ of the previous section. Each tuple m can be uniquely represented as a concatenation of indecomposable ones, $m = m^{(1)} * \dots * m^{(r)}$ and we write n in the form

$$n = n^{(1)} + p^{\ell(m^{(1)})} n^{(2)} + \ldots + p^{\ell(m^{(1)})+\ell(m^{(2)})+\dots+\ell(m^{(r-1)})} n^{(r)}$$

with $\ell(n^{(i)}) \le \ell(m^{(i)})$. Whenever $\ell(n^{(i)}) < \ell(m^{(i)})$ the corresponding summand $R^n_{m,\Lambda}(x)$ vanishes because in this case $\ell(m^{(i)}) \ge 2$, so the last element of $m^{(i)}$ is not zero and the product in the definition of $R^n_{m,\Lambda}(x)$ contains $R_s(\Lambda^0) = R_s(1) = 0$ for $s > 0$. Therefore we can assume $\ell(n^{(i)}) = \ell(m^{(i)})$. In this case $n = n^{(1)} * \cdots * n^{(r)}$, the corresponding summand is written as

$$R^n_{m,\Lambda}(x) \;=\; R^{n^{(1)}}_{m^{(1)},\Lambda}(x) R^{n^{(2)}}_{m^{(2)},\Lambda}(x^{p^{\ell(n^{(1)})}}) \cdots R^{n^{(r)}}_{m^{(r)},\Lambda}(x^{p^{\ell(n^{(1)})+\ell(n^{(2)})+\cdots+\ell(n^{(r-1)})}}),$$

and (i) follows. (ii) follows from Proposition 2 since $R^n_{m,\Lambda}(x) \;\equiv\; 0 \mod p^{|m|}$, and (iii) is due to the fact that $\mathrm{Newt}\Big(R^n_{m,\Lambda}\Big) \subset n\, \mathrm{Newt}(\Lambda)$. □

4. The case of one interior point

In this section we proceed to compute free terms of powers of $\Lambda(x) = \Lambda(x_1, \ldots, x_d)$. We will work under the assumption that the origin is the only interior integral point of the Newton polyhedron of Λ.

Proposition 4. *If $0 = (0, \ldots, 0)$ is the only interior integral point of* $\mathrm{Newt}(\Lambda)$, *then for any $r \ge 1$ and non-negative integers $n^{(1)}, \ldots, n^{(r)}$ one has*

$$\Big[I^{n^{(1)}}_\Lambda(x)\, I^{n^{(2)}}_\Lambda(x^{p^{\ell(n^{(1)})}}) \;\cdots\; I^{n^{(r)}}_\Lambda(x^{p^{\ell(n^{(1)})+\ell(n^{(2)})+\cdots+\ell(n^{(r-1)})}})\Big]_0 = \prod_{i=1}^{r} \Big[I^{n^{(i)}}_\Lambda\Big]_0.$$

Proof. Since $\mathrm{Newt}(I^{n^{(1)}}_\Lambda) \subset n^{(1)}\, \mathrm{Newt}(\Lambda)$ and $n^{(1)} < p^{\ell(n^{(1)})}$ we see that $N(I^{n^{(1)}}_\Lambda)$ does not contain points of the lattice $p^{\ell(n^{(1)})}\mathbb{Z}^d$ other then 0. Therefore the only contribution to the constant term on the left comes from the product

$$\begin{aligned}&\Big[I^{n^{(1)}}_\Lambda(x)\, I^{n^{(2)}}_\Lambda(x^{p^{\ell(n^{(1)})}}) \;\cdots\; I^{n^{(r)}}_\Lambda(x^{p^{\ell(n^{(1)})+\ell(n^{(2)})+\cdots+\ell(n^{(r-1)})}})\Big]_0 \\ &\qquad = \Big[I^{n^{(1)}}_\Lambda(x)\Big]_0 \Big[I^{n^{(2)}}_\Lambda(x^{p^{\ell(n^{(1)})}}) \;\cdots\; I^{n^{(r)}}_\Lambda(x^{p^{\ell(n^{(1)})+\ell(n^{(2)})+\cdots+\ell(n^{(r-1)})}})\Big]_0.\end{aligned}$$

Thus by induction on r we prove the statement. □

Together with Proposition 3 (i) this implies

Corollary. $\Big[\Lambda^n\Big]_0 \;=\; \sum_{n=n^{(1)}*\cdots*n^{(r)}} \prod_{i=1}^{r} \Big[I^{n^{(i)}}_\Lambda\Big]_0.$

Now we are in a position to prove Lemma 1.

Proof of Lemma 1. Put $c_n = \Big[I^n_\Lambda\Big]_0$. Then (4) is precisely the statement of the latter corollary, and (5) is given by Proposition 3 (ii). □

5. Proof of Theorem 1

Proof. We will prove (2). Fixing N and collecting coefficients near X^N on both sides we see that what we need to prove is

$$\sum_{\substack{n+pm=N \\ \ell(n)\le s+1,\, \ell(m)\le s-1}} b_n b_m \;\equiv\; \sum_{\substack{n'+pm'=N \\ \ell(n'),\, \ell(m')\le s}} b_{n'} b_{m'} \mod p^s$$

where the sums run over all pairs (n,m) and (n',m') that satisfy the respective conditions on the left and on the right. The sum of terms on the left with $\ell(n) \le s$ is equal to the sum of terms on the right with $\ell(m') \le s-1$ as the map $(n,m) \mapsto (n',m') = (n,m)$ provides a bijective correspondence. Therefore it remains to show that

$$\sum_{\substack{n+pm=N \\ \ell(n)=s+1,\,\ell(m)\le s-1}} b_n b_m \equiv \sum_{\substack{n'+m'p=N \\ \ell(n')\le s,\,\ell(m')=s}} b_{n'} b_{m'} \mod p^s \,. \tag{6}$$

Using decomposition (4) a product $b_n b_m$ becomes

$$b_n\, b_m \;=\; \sum_{\substack{n=n^{(1)}*\cdots*n^{(r)} \\ m=m^{(1)}*\cdots*m^{(l)}}} c_{n^{(1)}}\cdot\ldots\cdot c_{n^{(r)}}\cdot c_{m^{(1)}}\cdot\ldots\cdot c_{m^{(l)}}\,, \tag{7}$$

where we sum over all possible pairs of partitions of n and m. Let us say that a pair of partitions is *good* if for some $1 \le i < r$ one either has

$$\ell(n^{(1)}) + \ldots + \ell(n^{(i)}) \;=\; \ell(m^{(1)}) + \ldots + \ell(m^{(j)}) + 1$$

for some $0 \le j < l$ or

$$\ell(n^{(1)}) + \ldots + \ell(n^{(i)}) \ge \ell(m) + 1\,.$$

For a *good* pair of partitions we take the smallest such i and consider the pair (n',m') constructed as follows. If the former of the two options takes place then we put $n' = n^{(1)}*\cdots*n^{(i)}*m^{(j+1)}*\cdots*m^{(l)}$, $m' = m^{(1)}*\cdots*m^{(j)}*n^{(i+1)}*\cdots*n^{(r)}$. In the latter case let i' be the index of the last nonzero element of $n^{(1)},\ldots,n^{(i)}$ (they cannot be all zero as otherwise we would have chosen $i=1$). We put $n' = n^{(1)}*\cdots*n^{(i')}$, $m' = m*0*\cdots*0*n^{(i+1)}*\cdots*n^{(r)}$, where the number of zeroes to be inserted is $\ell(n^{(1)})+\ldots+\ell(n^{(i)})-\ell(m)-1$. It is not hard to see that $n+pm=N$ implies $n'+pm'=N$, and clearly $\ell(m') = \ell(n)-1 = s$. For $\ell(n')$ we either have $\ell(n') = \ell(m)+1 \le s$ or

$$\ell(n') = \ell(n^{(1)}) + \ldots + \ell(n^{(i')}) < \ell(n) = s+1\,.$$

Therefore (n',m') will occur in the right-hand sum in (6), and the same product of c's will enter decomposition (7) for $b_{n'}b_{m'}$. This way we obtain a bijective correspondence between *good* pairs of partitions of (n,m) in the left-hand sum in (6) and *good* pairs of partitions $n' = n'^{(1)}*\cdots*n'^{(r')}$, $m' = m'^{(1)}*\cdots*m'^{(l')}$ of (n',m') in the right-hand sum, where the latter pair is called *good* when for some $0 \le j < l'$ one either has

$$\ell(n'^{(1)}) + \ldots + \ell(n'^{(i)}) \;=\; \ell(m'^{(1)}) + \ldots + \ell(m'^{(j)}) + 1$$

for some $1 \le i < r'$ or

$$\ell(n') \le \ell(m'^{(1)}) + \ldots + \ell(m'^{(j)}) + 1\,.$$

It remains to show that products of c's corresponding to pairs of partitions on either side which are not *good* vanish modulo p^s. Let us first consider left-hand pairs. Suppose a pair of partitions $n = n^{(1)}*\cdots*n^{(r)}$, $m = m^{(1)}*\cdots*m^{(l)}$ is not *good*. There are $r-1$ possible sums $\ell(n^{(1)})+\ldots+\ell(n^{(i)})$ for $1 \le i < r$, l possible sums $\ell(m^{(1)})+\ldots+\ell(m^{(j)})+1$ for $0 \le j < l$ and $s-\ell(m)$ numbers k satisfying

$\ell(m)+1 \leq k < \ell(n) = s+1$. As the pair of partitions is not *good* all these numbers must be distinct. Since they all belong to the range between 1 and s, we then have $(r-1)+l+(s-\ell(m)) \leq s$, i.e. $r+l \leq \ell(m)+1$. Using (5) we conclude that

$$c_{n^{(1)}} \cdot \ldots \cdot c_{n^{(r)}} \cdot c_{m^{(1)}} \cdot \ldots \cdot c_{m^{(l)}} \equiv 0 \mod p^a$$

where

$$a = \sum_{i=1}^{r} \big(\ell(n^{(i)})-1\big) + \sum_{j=1}^{l} \big(\ell(m^{(j)})-1\big) = \ell(n)+\ell(m)-r-l$$
$$\geq \ell(n)-1 = s.$$

Similarly, consider a pair of partitions $n' = n'^{(1)} * \cdots * n'^{(r')}$, $m' = m'^{(1)} * \cdots * m'^{(l')}$ which is not *good*. There are now $r'-1$ possible sums $\ell(n'^{(1)}) + \ldots + \ell(n'^{(i)})$ for $1 \leq i < r'$, l' possible sums $\ell(m'^{(1)})+\ldots+\ell(m'^{(j)})+1$ for $0 \leq j < l'$ and $s+1-\ell(n')$ numbers k satisfying $\ell(n') \leq k < \ell(m')+1 = s+1$. All these numbers are distinct and belong to the range between 1 and s, hence we have $r'-1+l'+(s+1-\ell(n')) \leq s$, so $r'+l' \leq \ell(n')$. Using (5) we conclude that

$$c_{n'^{(1)}} \cdot \ldots \cdot c_{n'^{(r')}} \cdot c_{m'^{(1)}} \cdot \ldots \cdot c_{m'^{(l')}} \equiv 0 \mod p^a$$

where

$$a = \sum_{i=1}^{r'} \big(\ell(n'^{(i)})-1\big) + \sum_{j=1}^{l'} \big(\ell(m'^{(j)})-1\big) = \ell(n')+\ell(m')-r'-l'$$
$$\geq \ell(m') = s.$$

□

The reader could deduce congruences (3) from Lemma 1 in a similar way.

Acknowledgment

We want to express our gratitude to Vasily Golyshev for introducing both authors to this topic and for discussions which motivated our work all the time.

References

[1] B. Dwork, *p-adic cycles*, Publ. Math. IHES 37, 1969, pp. 27–116
[2] B. Dwork, *A deformation theory for the zeta function of a hypersurface*, Proc. Int. Cong. Math. Stockholm, 1962, pp. 247–259
[3] N. Katz, *Travaux de Dwork*, Séminaire N. Bourbaki, 1971-72, no. 409, pp. 167–200
[4] K. Samol, D. van Straten, *Dwork congruences and reflexive polytopes*, arXiv:0911.0797v1, 2009, pp. 1–14