A Matrix Version of Dwork's Congruences

Frits Beukers

Abstract In this article we give an example of a matrix version of the famous congruence for hypergeometric functions found by Dwork in 'p-adic cycles'.

1 Introduction

In this paper we shall deal with results of the following type. Let $F(t)$ be an infinite power series with constant term 1 and coefficients in $\mathbb{Z}_p$, the p-adic numbers. Denote by $F_m(t)$ its m-th truncation, i.e. all terms of degree $\geq m$ in $F(t)$ are deleted. We shall be interested whether there are hypergeometric series $F(t)$ for which

$$\frac{F(t)}{F(t^p)} \equiv \frac{F_{p^s}(t)}{F_{p^{s-1}}(t^p)} (\bmod\ p^s) \tag{1}$$

for all $s \geq 1$. The first such result was given by Dwork in 'p-adic cycles', [3], for the case of $F(t) = F(1/2, 1/2; 1|t)$. The proof of this result is based on a p-adic study of the coefficients of $F(1/2, 1/2; 1|t)$. Using [3, Cor 1] and [3, Thm 3] one can generalize this approach to other hypergeometric functions whose monodromy around 0 is unipotent (i.e. all β-parameters are 1). The goal of the present paper is to provide a more geometric approach to Dwork's congruences based on the papers [1] and [2] (Dwork crystals I and II), written jointly with Masha Vlasenko. In it we give an elementary approach to the construction of the so-called unit root crystal in Dwork's p-adic theory of zeta-functions of algebraic varieties. As application we present in this paper some hypergeometric examples of (1) in Sect. 3. In Sect. 5 we present main result of this paper,

Work supported by the Netherlands Organisation for Scientific Research (NWO), grant TOP1EW.15.313.

F. Beukers (✉)
Utrecht University, Utrecht, The Netherlands
e-mail: f.beukers@uu.nl

A. Bostan and K. Raschel (eds.), *Transcendence in Algebra, Combinatorics, Geometry and Number Theory*, Springer Proceedings in Mathematics & Statistics 373,
https://doi.org/10.1007/978-3-030-84304-5_2

Theorem 5.1, containing an example of a matrix version of Dwork's congruence. Its proof requires some ideas in addition to [1] and [2].

2 Summary of [1] and [2]

Let R be a characteristic zero domain and p an odd prime such that $\cap_{s\geq 1} p^s R = \{0\}$. Suppose that R is p-adically complete. Let $f \in R[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a Laurent polynomial and $\Delta \subset \mathbb{R}^n$ its Newton polytope. Let Δ° be its interior. Consider the R-module Ω_f° of differential forms generated over R by

$$\omega_{\mathbf{u}} := (k-1)! \frac{\mathbf{x}^{\mathbf{u}}}{f(\mathbf{x})^k} \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}, \quad \mathbf{u} \in k\Delta^\circ$$

for all $k \geq 1$. Contrary to [1] and [2] we have now written the elements of Ω_f as differential forms. Let us abbreviate $\frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$ to $\frac{d\mathbf{x}}{\mathbf{x}}$.

Differential forms in Ω_f° can be expanded as formal Laurent series. To that end we choose a vertex $\mathbf{b}$ of Δ and obtain a Laurent expansion with support in $C(\Delta - \mathbf{b})$, the positive cone generated by the vectors in $\Delta - \mathbf{b}$, and coefficients in R of the form

$$\sum_{\mathbf{k} \in C(\Delta - \mathbf{b})} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \frac{d\mathbf{x}}{\mathbf{x}}, \quad a_{\mathbf{k}} \in R.$$

We denote such forms by Ω_{formal}. The exact forms are denoted by $d\Omega_{\text{formal}}$. We call them formally exact forms and they are characterized by the following lemma of Katz, [4, Lemma 5.1].

Lemma 2.1. *A series* $\sum_{\mathbf{k} \in C(\Delta - \mathbf{b})} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \frac{d\mathbf{x}}{\mathbf{x}}$ *is a formal derivative if and only if*

$$a_{\mathbf{k}} \equiv 0 (\text{mod } p^{\text{ord}_p(\mathbf{k})}) \quad \textit{for all } \mathbf{k}.$$

Here $\text{ord}_p(k)$ *denotes the* p*-adic valuation of* k *and* $\text{ord}_p(\mathbf{k}) = \min(\text{ord}_p(k_1), \dots, \text{ord}_p(k_n))$.

We define the Cartier operator $\mathscr{C}_p$ on Ω_{formal} by

$$\mathscr{C}_p \left(\sum_{\mathbf{k}} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \frac{d\mathbf{x}}{\mathbf{x}} \right) := \sum_{\mathbf{k}} a_{p\mathbf{k}} \mathbf{x}^{\mathbf{k}} \frac{d\mathbf{x}}{\mathbf{x}}. \tag{2}$$

Using $\mathscr{C}_p$ we have an alternative characterization of formally exact forms which is a direct consequence of Lemma 2.1.

Lemma 2.2. *A series* $h \in \Omega_{\text{formal}}$ *is a formal derivative if and only if* $\mathscr{C}_p^s(h) \equiv 0 (\text{mod } p^s)$ *for all integers* $s \geq 1$.

When applied to a rational differential form $\mathscr{C}_p$ acts as

$$\mathscr{C}_p\left(S(\mathbf{x})\frac{d\mathbf{x}}{\mathbf{x}}\right) = \sum_{\mathbf{y}:\mathbf{y}^p=\mathbf{x}} S(\mathbf{y})\frac{d\mathbf{y}}{\mathbf{y}}.$$

The summation extends over all $y_i = \zeta_i x_i^{1/p}$, $i = 1, \ldots, n$, where each ζ_i runs over all p-th roots of unity. So we see that $\mathscr{C}_p$ sends rational differential forms to rational differential forms. Unfortunately, Ω_f° is not sent to itself. But we have something that comes close. Define the p-adic completion

$$\widehat{\Omega}_f^\circ := \lim_{\leftarrow} \Omega_f^\circ / p^s \Omega_f^\circ.$$

Fix a Frobenius lift σ on R: this is a ring endomorphism $\sigma : R \to R$ such that $\sigma(r) \equiv r^p (\mathrm{mod}\ p)$ for every $r \in R$. We have

Proposition 2.3. *If $p > 2$ then $\mathscr{C}_p(\Omega_f^\circ) \subset \widehat{\Omega}_{f^\sigma}^\circ$.*

The proof is given in [1, Prop 3.3] and consists of a straightforward computation ending with a p-adic expansion in $\widehat{\Omega}_{f^\sigma}^\circ$.

We shall be interested in $U_f^\circ := \widehat{\Omega}_f^\circ \cap d\Omega_{\mathrm{formal}}$. These are differential forms that are not necessarily exact but become exact when embedded in the formal expansions. Katz refers to them as 'forms that die on formal expansion', [4, Thm 6.2(1.b)]. In [1, Prop 4.2] we find a characterization of the elements of U_f° without any reference to formal expansion.

Proposition 2.4. *With the notations as above we have*

$$U_f^\circ = \{\omega \in \widehat{\Omega}_f^\circ \mid \mathscr{C}_p^s(\omega) \equiv 0 (\mathrm{mod}\ p^s \widehat{\Omega}_{f^{\sigma^s}}^\circ)\ \textit{for all}\ s \geq 1\}.$$

We now come to one of the main results in [1, Thm 4.3]. Let $h = |\Delta^\circ \cap \mathbb{Z}^n|$. Define the Hasse-Witt matrix β_p as the $h \times h$-matrix given by

$$(\beta_p)_{\mathbf{u},\mathbf{v}} = \text{coefficient of } \mathbf{x}^{p\mathbf{u}-\mathbf{v}} \text{ of } f(\mathbf{x})^{p-1}, \quad \mathbf{u}, \mathbf{v} \in \Delta^\circ \cap \mathbb{Z}^n$$

Theorem 2.5. *Suppose* $\det(\beta_p)$ *is invertible in R. Then $\widehat{\Omega}_f^\circ / U_f^\circ$ is a free R-module of rank h with basis $\frac{\mathbf{x}^\mathbf{u}}{f}\frac{d\mathbf{x}}{\mathbf{x}}$, $\mathbf{u} \in \Delta^\circ \cap \mathbb{Z}^n$.*

The remainder of [1] and [2] is then devoted to the construction of p-adic approximations to the $h \times h$-matrix of the Cartier operator. In [2] we give special attention to those approximations that give rise to congruences of the form (1) (in case $h = 1$) and higher.

3 First Examples

In [5] we find a very general theorem providing congruences of the form (1).

Theorem 3.1 (Mellit-Vlasenko). *Let $g(\mathbf{x}) \in \mathbb{Z}_p[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a Laurent polynomial in the variables $x_1, \dots, x_n$. Suppose that the Newton polytope Δ of g has the origin as unique interior lattice point. For every integer $r \geq 0$ denote by f_r the constant term of $g(\mathbf{x})^r$ and define $F(t) = \sum_{r \geq 0} f_r t^r$. Then the congruences (1) hold for all $s \geq 1$.*

In [2, (7)] there is a stronger result with an entirely different proof.

Theorem 3.2 (Beukers-Vlasenko). *With the same notations as in Theorem 3.1 we have*

$$\frac{F(t)}{F(t^p)} \equiv \frac{F_{mp^s}(t)}{F_{mp^{s-1}}(t^p)} \pmod{p^s} \tag{3}$$

for all $m, s \geq 1$.

Here is an application.

Corollary 3.3. *Let $k \geq 2$ be an integer and p an odd prime not dividing k. Then (1) holds for the hypergeometric series*

$$_{k-1}F_{k-2}(1/k, 2/k, \dots, (k-1)/k; 1, 1, \dots, 1|t).$$

Proof. Consider

$$g = \frac{1}{k}\left(x_1 + \cdots + x_{k-1} + \frac{1}{x_1 \cdots x_{k-1}}\right).$$

A simple calculation show that f_r is zero if k does not divide r and equal to

$$\frac{1}{k^{kl}} \frac{(kl)!}{(l!)^k} = \frac{(1/k)_l}{l!} \frac{(2/k)_l}{l!} \cdots \frac{((k-1)/k)_l}{l!}$$

if $r = kl$. Hence

$$F(t) = {}_{k-1}F_{k-2}(1/k, 2/k, \dots, (k-1)/k; 1, 1, \dots, 1|t^k).$$

Now apply Theorem 3.2 with $m = k$ and replace t^k by t. □

Here is another variation which generalizes Dwork's example

Corollary 3.4. *Let $k \geq 2$ be an integer and p an odd prime. Then (1) holds for the hypergeometric series*

$$_{k-1}F_{k-2}(1/2, 1/2, \dots, 1/2; 1, 1, \dots, 1|t).$$

Proof. Consider

$$g = 2^{-k}\left(x_1 + \frac{1}{x_1}\right)\cdots\left(x_k + \frac{1}{x_k}\right).$$

A simple calculation shows that f_r is zero if r is odd and equal to

$$\left(\frac{(1/2)_l}{l!}\right)^k$$

if $r = 2l$. Hence

$$F(t) = {}_{k-1}F_{k-2}(1/2, \dots, 1/2; 1, 1, \dots, 1|t^2).$$

Now apply Theorem 3.2 with $m = 2$ and replace t^2 by t. □

4 One Variable Polynomials

Let again R be a characteristic zero ring, p an odd prime such that $\cap_{s\geq 1} p^s R = \{0\}$ and suppose R is p-adically complete. Let $\sigma : R \to R$ be a Frobenius lift. It turns out that in the case of one variable polynomials f the theory sketched in Sect. 2 has a very nice simplification that we like to present for general monic $f \in R[x]$ with $f(0) \neq 0$. Let d be the degree of f. We suppose that $d \geq 2$ and that the discriminant of f is invertible in R. The space Ω_f° is given by $\mathscr{O}_f^\circ dx$ where $\mathscr{O}_f^\circ$ is the R-module generated by the forms $l!\frac{x^k}{f^{l+1}}$ with $0 \leq k \leq d(l+1) - 2$. Similarly we define $\mathscr{O}_f$ in the same way but with the inequalities $0 \leq k \leq d(l+1) - 1$. The exact forms in Ω_f° are then given by $d\mathscr{O}_f$. We call them *rational exact forms*.

We define $\mathscr{O}_{\text{formal}} = \frac{1}{x}R[\![1/x]\!]$ and $\Omega_{\text{formal}} = \frac{1}{x}\mathscr{O}_{\text{formal}}dx$. We embed Ω_f° in Ω_{formal} by expansion in powers of $1/x$. The *formally exact forms* are defined by $d\mathscr{O}_{\text{formal}}$.

The interior of the Newton polytope is $\Delta^\circ = (0, d)$ and the cardinality of $\Delta^\circ \cap \mathbb{Z}$ is $d - 1$. So, letting p be an odd prime, the Hasse-Witt matrix $\beta_p(t)$ is a $(d-1) \times (d-1)$-matrix. It turns out that $\det(\beta_p) \equiv \text{disc}(f)^{p-1} (\text{mod } p)$, where $\text{disc}(f)$ is the discriminant of f. By p-adic completeness of R and invertibility of $\text{disc}(f)$ in R we find that $\det(\beta_p)$ is invertible in R. According to Theorem 11 in Dwork crystals I, [1], we know that $\widehat{\Omega}_f^\circ / d\mathscr{O}_{\text{formal}}$ is a free rank $d-1$ module over R with basis $dx/f, x\,dx/f, \dots, x^{d-2}dx/f$.

It turns out that in the case $n = 1$ formally exact forms coincide with rational exact forms. More precisely,

Proposition 4.1. *Let $f \in R[x]$ be a monic polynomial and suppose that its discriminant is invertible in R. Then $\Omega_f^\circ \cap d\mathscr{O}_{\text{formal}} = d\mathscr{O}_f$.*

Proof. Clearly $d\mathcal{O}_f \subset d\mathcal{O}_{\text{formal}}$. We first show that every $\omega \in \Omega_f^\circ$ is equivalent modulo $d\mathcal{O}_f$ to a form $Q(x)dx/f$ with $Q(x) \in R[x]$ of degree $\le d-2$. To that end we use the one variable version of the Griffiths reduction procedure. Since p does not divide $\text{disc}(f)$, to every $Q(x) \in R[x]$ of degree $\le N$ there exist polynomials $A, B \in R[x]$ of degrees $\le d-1$ and $\le \max(d-2, N-d)$ respectively, such that $Q = Af' + Bf$.

Let us start with a form $l!Q(x)dx/f^{l+1}$ with $\deg(Q) \le (l+1)d - 2$ and $l > 0$. Write $Q = Af' + Bf$ with $\deg(A) \le d-1$, $\deg(B) \le ld-2$. Then we obtain

$$\begin{aligned} l!\frac{Q(x)}{f^{l+1}}dx &= l!\frac{Af'}{f^{l+1}}dx + l!\frac{B}{f^l}dx \\ &= -d\left((l-1)!\frac{A}{f^l}\right) + (l-1)!\frac{A'}{f^l}dx + l!\frac{B}{f^l}dx \\ &\equiv (l-1)!\frac{lB + A'}{f^l}dx (\text{mod } d\mathcal{O}_f). \end{aligned}$$

Note that $\deg(lB + A') \le ld - 2$. By repeating this procedure we see that any $\omega \in \Omega_f^\circ$ is equivalent modulo $d\mathcal{O}_f$ to a form Qdx/f with $Q \in R[x]$ of degree $\le d-2$.

The second part of our proof consists of showing that $Qdx/f \in d\mathcal{O}_{\text{formal}}$ implies that $Q = 0$. Suppose that

$$\frac{Qdx}{f} = d\left(\sum_{n\ge 0}\frac{a_n}{x^n}\right) = \sum_{n\ge 1} -\frac{na_n}{x^{n+1}}dx.$$

From this we see that the coefficient of dx/x^{mp^s+1} in the $1/x$-expansion of Qdx/f is divisible by p^s for any $m, s \ge 0$. Let K be the splitting field of f over R and let $\alpha_1, \ldots, \alpha_d \in K$ be the zeros of f. Then there exist $A_1, \ldots, A_d$ in $R[\alpha_1, \ldots, \alpha_d]$ such that

$$\text{disc}(f)\frac{Qdx}{f} = \sum_{i=1}^{d}\frac{A_i dx}{x - \alpha_i} = \sum_{n\ge 0}(A_1\alpha_1^n + \cdots + A_d\alpha_d^n)\frac{dx}{x^{n+1}}.$$

We now know that $A_1\alpha_1^{mp^s} + \cdots + A_d\alpha_d^{mp^s}$ is divisible by p^s for all $m \ge 0$. In particular for $m = 0, 1, \ldots, d-1$. Now note that

$$\begin{aligned} \det((\alpha_i^{mp^s})_{i=1,\ldots,d;m=0,\ldots,d-1}) &= \prod_{i<j}(\alpha_i^{p^s} - \alpha_j^{p^s}) \\ &\equiv \prod_{i<j}(\alpha_i - \alpha_j)^{p^s} \equiv \text{disc}(f)^{p^s} (\text{mod } p), \end{aligned}$$

which is a unit in R. We conclude that $A_i \equiv 0 (\text{mod } p^s)$ for all i and s. Hence $A_i = 0$ for all i and we conclude $Q(x) = 0$, as asserted. □

An immediate corollary is its extension to p-adic completions. Denote $\widehat{\Omega}_f^\circ$ as before and similarly $\widehat{\mathscr{O}}_f$. Then we find,

Proposition 4.2. *Let $f \in R[x]$ be a monic polynomial and suppose that its discriminant is invertible in R. Then $U_f^\circ = \widehat{\Omega}_f^\circ \cap d\mathscr{O}_{\text{formal}} = d\widehat{\mathscr{O}}_f$.*

The operator $\mathscr{C}_p$ is essentially a lift of a Cartier operator which is only well-defined in characteristic p. In [1] and [2] it sufficed to use only the operator $\mathscr{C}_p$ defined above. However, as a new ingredient, we need to consider other lifts. Let $a \in \mathbb{Z}_p$. Define $\mathscr{C}_p^a$ as the operator with the property that $\mathscr{C}_p^a((x-a)^{k-1}dx) = (x-a)^{k/p-1}dx$ if p divides k and 0 if not. In general it acts on rational differential forms as

$$\mathscr{C}_p^a\left(S(x)\frac{dx}{x}\right) = \sum_{y:(y-a)^p=x-a} S(y)\frac{dy}{y}.$$

So we sum over $y = a + \zeta(x-a)^{1/p}$ where ζ runs over the p-th roots of unity. We can compare $\mathscr{C}_p$ and $\mathscr{C}_p^a$ by looking at their action on Ω_{formal}.

Proposition 4.3. *We have $\mathscr{C}_p^a(\Omega_f^\circ) \subset \widehat{\Omega}_{f^\sigma}^\circ$ and*

$$\mathscr{C}_p(\omega) \equiv \mathscr{C}_p^a(\omega) (\text{mod } pd\widehat{\mathscr{O}}_{f^\sigma}) \tag{4}$$

for all $\omega \in \Omega_f^\circ$.

Proof. The fact that the image of $\mathscr{C}_p^a$ lies in $\widehat{\Omega}_{f^\sigma}^\circ$ follows along the same lines as in the proof of [1, Prop 3.3]. Clearly we have $R[\![1/x]\!] \cong R[\![1/(x-a)]\!]$ through the expansion $\frac{1}{x-a} = \sum_{n\ge0} \frac{a^n}{x^{n+1}}$. Let us prove our second assertion for $\omega_k = (x-a)^{-k-1}dx$ for $k \ge 1$. The full statement then follows by linearity.

Observe that

$$\omega_k = (x-a)^{-k-1}dx = -d\left(\frac{1}{k}(x-a)^{-k}\right).$$

If k is not divisible by p then clearly $\omega_k \in d\mathscr{O}_{\text{formal}}$. Since $\mathscr{C}_p(d\mathscr{O}_{\text{formal}}) \subset pd\mathscr{O}_{\text{formal}}$ we get that $\mathscr{C}_p(\omega_k) \equiv 0 (\text{mod } pd\mathscr{O}_{\text{formal}})$. We have trivially $\mathscr{C}_p^a(\omega_k) = 0$. This proves our statement for k not divisible by p. Suppose now that p divides k. Then

$$\frac{1}{k}(x-a)^{-k} \equiv \frac{1}{k}(x^p-a)^{-k/p} (\text{mod } \mathscr{O}_{\text{formal}})$$

hence, after taking differentials,

$$(x-a)^{-k-1}dx \equiv (x^p-a)^{-k/p-1}x^{p-1}dx (\text{mod } d\mathscr{O}_{\text{formal}}).$$

Application of $\mathscr{C}_p$ gives $\mathscr{C}_p(\omega_k) \equiv \omega_{k/p} (\text{mod } pd\mathscr{O}_{\text{formal}})$. Note that $\omega_{k/p} = \mathscr{C}_p^a(\omega_k)$ when p divides k. Thus we conclude that

$$\mathscr{C}_p(\omega_k) \equiv \mathscr{C}_p^a(\omega_k) (\bmod\ pd\mathscr{O}_{\text{formal}}).$$

By linearity this congruence holds for all $\omega \in \Omega_f^\circ$.

It remains to see that we can replace $pd\mathscr{O}_{\text{formal}}$ by $pd\widehat{\mathscr{O}}_f$. From Proposition 3.6 in [1] it follows that to any $\omega \in \widehat{\Omega}_f^\circ$ there exists $\omega_1 \in \widehat{\Omega}_{f^\sigma}^\circ$ and a polynomial $A(a, \omega)$ such that $\mathscr{C}_p^a(\omega) = \frac{A(a,\omega)}{f^\sigma} + p\omega_1$. Since $\mathscr{C}_p^a(\omega) - \mathscr{C}_p^0(\omega) \in pd\mathscr{O}_{\text{formal}}$ it follows that $A(a, \omega) - A(0, \omega)$ is divisible by p. Hence

$$\frac{1}{p}(\mathscr{C}_p^a(\omega) - \mathscr{C}_p^0(\omega)) \in \widehat{\Omega}_{f^\sigma}^\circ \cap d\mathscr{O}_{\text{formal}} = d\widehat{\mathscr{O}}_{f^\sigma}.$$

The latter equality follows from Proposition 4.2. □

5 A Matrix Example

The examples in the Sect. 3 are all related to the case $h = 1$, one interior lattice point of the Newton polytope Δ. In this section we consider an example of rank $h = 2$.

Theorem 5.1. *Let*

$$\mathscr{Y}(t) = \begin{pmatrix} F(1/3, 2/3, 1/2|t^2) & -\frac{1}{3}tF(7/6, 5/6, 3/2|t^2) \\ -\frac{2}{3}tF(2/3, 4/3, 3/2|t^2) & F(1/6, 5/6, 1/2|t^2) \end{pmatrix}.$$

Denote by $\mathscr{Y}_m(t)$ the m-th truncated version of $\mathscr{Y}(t)$, i.e. we drop all term starting with t^m. Then, for all primes $p > 3$ and all $m, s \geq 1$ we have

$$\mathscr{Y}_{mp^s}(t) \begin{pmatrix} \epsilon_p & 0 \\ 0 & 1 \end{pmatrix} \mathscr{Y}_{mp^{s-1}}(t^p)^{-1} \equiv \mathscr{Y}(t) \begin{pmatrix} \epsilon_p & 0 \\ 0 & 1 \end{pmatrix} \mathscr{Y}(t^p)^{-1} (\bmod\ p^s).$$

Here $\epsilon_p = 1$ if 3 is a square modulo p and -1 if not.

For the proof of this theorem, given at the end of this section, we require the one variable polynomial $f = x^3 - x - t \in R[x]$ with $R = \mathbb{Z}_p[\![t]\!]$, where p is a prime with $p > 3$. As Frobenius lift we take $g(t)^\sigma = g(t^p)$ for all $g(t) \in R$. The discriminant of f equals to $4 - 27t^2$, and hence it is invertible in R.

We define the 2×2-matrix Λ_p with entries in R by

$$\mathscr{C}_p \begin{pmatrix} dx/f \\ xdx/f \end{pmatrix} \equiv \Lambda_p \begin{pmatrix} dx/f^\sigma \\ xdx/f^\sigma \end{pmatrix} (\bmod\ d\widehat{\mathscr{O}}_f). \tag{5}$$

The relation of Λ_p with hypergeometric functions is obtained by period maps. To that end we consider

$$l!\frac{x^{k-1}dx}{f^{l+1}} = l!\frac{x^{k-1}dx}{(x^3-x)^{l+1}} \sum_{r\geq 0} \binom{r+l}{l} \frac{t^r}{(x^3-x)^r},$$

and then take termwise the residue at $x = 0$. We could rephrase this procedure by saying that we expand $x^{k-1}dx/f^{l+1}$ as two-sided Laurent series in $R[\![x, t/x]\!]$ and then take the residue at $x = 0$. Similarly we can take residues at $x = \pm 1$ (i.e. by expanding in Laurent series in $x \mp 1$). The result is again a power series in t. As long as $0 < k < 3(l+1)$ the terms of the series have no residue at ∞ and therefore the sum of the residues at $0, 1, -1$ of the series is 0. We carry out the residue computations for $l = 0, k = 1, 2$. A straightforward calculation shows that

$$\mathrm{res}_{x=0} \frac{dx}{(x^3-x)^{r+1}} = \begin{cases} 0 & \text{if } r \text{ is odd} \\ -\binom{3n}{n} & \text{if } r = 2n \end{cases}$$

$$\mathrm{res}_{x=0} \frac{xdx}{(x^3-x)^{r+1}} = \begin{cases} 0 & \text{if } r \text{ is even} \\ \binom{3n+1}{n} & \text{if } r = 2n+1 \end{cases}.$$

Denote $\mathrm{res}_{\pm}\omega = \mathrm{res}_{x=1}\omega - \mathrm{res}_{x=-1}\omega$. Then we obtain

$$\mathrm{res}_{\pm} \frac{dx}{(x^3-x)^{r+1}} = \begin{cases} 0 & \text{if } r \text{ is even} \\ -\frac{3}{2}\frac{(7/6)_n(5/6)_n}{(3/2)_n n!}\left(\frac{27}{4}\right)^n & \text{if } r = 2n+1 \end{cases}$$

$$\mathrm{res}_{\pm} \frac{xdx}{(x^3-x)^{r+1}} = \begin{cases} 0 & \text{if } r \text{ is odd} \\ \frac{(1/6)_n(5/6)_n}{(1/2)_n n!}\left(\frac{27}{4}\right)^n & \text{if } r = 2n \end{cases}.$$

Let us denote the period map obtained by taking *minus* the residue at 0 by ρ_0 and the one by taking the difference of the residues at ± 1 by $\rho_{\pm}$. We summarize

$$\rho_0\,(dx/f) = F(1/3, 2/3, 1/2|27t^2/4).$$

$$\rho_0\,(xdx/f) = -tF(2/3, 4/3, 3/2|27t^2/4).$$

$$\rho_{\pm}\,(dx/f) = -\frac{3}{2}tF(7/6, 5/6, 3/2|27t^2/4).$$

$$\rho_{\pm}\,(xdx/f) = F(1/6, 5/6, 1/2|27t^2/4).$$

A crucial property of $\rho_0, \rho_{\pm}$ is that they vanish on exact forms, i.e. $d\widehat{\mathcal{O}}_f$. This is because residues of exact forms are zero, which is a special case of [2, Prop 2.2].

Proposition 5.2. *For every $\omega \in \widehat{\Omega}_f^{\circ}$ we have $\rho_0(\mathscr{C}_p(\omega)) = \rho_0(\omega)$ and $\rho_{\pm}(\mathscr{C}_p(\omega)) = \rho_{\pm}(\omega)$.*

Proof. Let $\omega \in \widehat{\Omega}_f^\circ$. Expand it in $R[\![x, t/x]\!]dx$. The value of ρ_0 is minus the coefficient of dx/x. By definition of $\mathscr{C}_p$ this value is the same for $\mathscr{C}_p(\omega)$, hence our first assertion follows. Similarly we can see that the residue at 1, which we denote by ρ_1, has the property $\rho_1(\mathscr{C}_p^1(\omega)) = \rho_1(\omega)$. It follows from Proposition 4.3 that $\mathscr{C}_p^1(\omega) \equiv \mathscr{C}_p(\omega) (\mathrm{mod}\ d\widehat{\mathscr{O}}_f)$. Hence $\rho_1(\mathscr{C}_p(\omega)) = \rho_1(\omega)$. The same result holds of course for $\rho_\pm = \rho_1 - \rho_{-1}$. □

Corollary 5.3. *Let*

$$Y(t) = \begin{pmatrix} F(1/3, 2/3; 1/2|27t^2/4) & -\frac{3}{2}tF(7/6, 5/6; 3/2|27t^2/4) \\ -tF(2/3, 4/3; 3/2|27t^2/4) & F(1/6, 5/6; 1/2|27t^2/4) \end{pmatrix}.$$

Let Λ_p *be the* 2×2 *cartier-matrix in (5). Then*

$$\Lambda_p = Y(t)Y(t^p)^{-1}.$$

Proof. We start with the equality (5), apply ρ_0 and use $\rho_0 \circ \mathscr{C}_p = \rho_0$ to obtain

$$\begin{pmatrix} \rho_0(dx/f) \\ \rho_0(xdx/f) \end{pmatrix} = \Lambda_p \begin{pmatrix} \rho_0(dx/f^\sigma) \\ \rho_0(xdx/f^\sigma) \end{pmatrix}.$$

Similarly we obtain

$$\begin{pmatrix} \rho_\pm(dx/f) \\ \rho_\pm(xdx/f) \end{pmatrix} = \Lambda_p \begin{pmatrix} \rho_\pm(dx/f^\sigma) \\ \rho_\pm(xdx/f^\sigma) \end{pmatrix}.$$

Our corollary follows from the above evaluations of the periods. □

In order to get Dwork type congruences we also need to introduce a suitable 'period map mod m'. By that we mean an R-linear map $\rho : \widehat{\Omega}_f \to R$ such that $\rho(\widehat{\Omega}_f \cap d\mathscr{O}_{\mathrm{formal}}) \subset mR$ and $\delta \circ \rho \equiv \rho \circ \delta (\mathrm{mod}\ mR)$ for any derivation δ on R.

For our purposes we use a slight generalization of the period maps we considered in [2, Section 5]. We define $\rho_{0,m}$ by

$$\rho_{0,m}\omega = \rho_0 \left(1 - \frac{t^m}{(x^3 - x)^m}\right)\omega. \tag{6}$$

Similarly we define $\rho_{1,m}$, $\rho_{-1,m}$ and the difference $\rho_{\pm,m}$. As an illustration we elaborate $\rho_{0,m}(dx/f)$. We get

$$\begin{aligned}\rho_{0,m}(dx/f) &= -\mathrm{res}_{x=0}\left(1-\frac{t^m}{(x^3-x)^m}\right)\frac{dx}{x^3-x-t}\\ &= -\mathrm{res}_{x=0}\frac{1}{(x^3-x)^m}\sum_{r=0}^{m-1}(x^3-x)^{m-1-r}t^r\,dx\\ &= -\mathrm{res}_{x=0}\sum_{r=0}^{m-1}\frac{t^r\,dx}{(x^3-x)^{r+1}}\\ &= \sum_{2n<m}\binom{3n}{n}t^{2n}.\end{aligned}$$

The latter polynomial is the truncation of $F(1/3, 2/3, 1/2|27t^2/4)$ truncated at the degree m term. Denote the truncation at degree m of a power series $g(t)$ by $g(t)_m$. Then we obtain

$$\rho_{0,m}\,(dx/f) = F(1/3, 2/3, 1/2|27t^2/4)_m.$$

$$\rho_{0,m}\,(xdx/f) = -(tF(2/3, 4/3, 3/2|27t^2/4))_m.$$

$$\rho_{\pm,m}\,(dx/f) = -\frac{3}{2}(tF(7/6, 5/6, 3/2|27t^2/4))_m.$$

$$\rho_{\pm,m}\,(xdx/f) = F(1/6, 5/6, 1/2|27t^2/4)_m.$$

Lemma 5.4. *We have* $\rho_{0,m}(d\widehat{\mathscr{O}}_f) \equiv 0(\mathrm{mod}\ m)$ *and* $\rho_{\pm,m}(d\widehat{\mathscr{O}}_f) \equiv 0(\mathrm{mod}\ m)$.

Secondly, for any $m \geq 1$ *divisible by* p *we have* $\rho_{0,m} \equiv \rho^{\sigma}_{0,m/p} \circ \mathscr{C}_p(\mathrm{mod}\ p^{\mathrm{ord}_p(m)})$ *and* $\rho_{\pm,m} \equiv \rho^{\sigma}_{\pm,m/p} \circ \mathscr{C}_p(\mathrm{mod}\ p^{\mathrm{ord}_p(m)})$. *Here* $\rho^{\sigma}_{0,m}$ *is defined as in equation (6) but with* t *replaced by* t^p. *Similarly for* $\rho^{\sigma}_{\pm,m}$.

Proof. For any $G \in \widehat{\mathscr{O}}_f$ we have

$$\begin{aligned}\rho_{0,m}dG &= -\text{coefficient of } \tfrac{dx}{x} \text{ in } \left(1-\left(\frac{t}{x^3-x}\right)^m\right)dG\\ &\equiv -\text{coefficient of } \tfrac{dx}{x} \text{ in } d\left(1-\left(\frac{t}{x^3-x}\right)^m\right)G \equiv 0(\mathrm{mod}\ m).\end{aligned}$$

The applicability of ρ_0 requires that we consider expansions as doubly infinite Laurent series in $R[\![x, t/x]\!]$. For $\rho_{1,m}$ the proof runs similarly.

For the proof of the second part let $\omega \in \widehat{\Omega}_f$. Then we have

$$\begin{aligned}\rho_{0,m}(\omega) &= -\text{coefficient of } \tfrac{dx}{x} \text{ in } \left(1-\left(\frac{t}{x^3-x}\right)^m\right)\omega\\ &\equiv -\text{coefficient of } \tfrac{dx}{x} \text{ in } \left(1-\left(\frac{t^p}{x^{3p}-x^p}\right)^{m/p}\right)\omega \pmod{p^{\mathrm{ord}_p(m)}}\\ &\equiv -\text{coefficient of } \tfrac{dx}{x} \text{ in } \mathscr{C}_p\left(1-\left(\frac{t^p}{x^{3p}-x^p}\right)^{m/p}\right)\omega \pmod{p^{\mathrm{ord}_p(m)}}\\ &\equiv -\text{coefficient of } \tfrac{dx}{x} \text{ in } \left(1-\left(\frac{t^p}{x^3-x}\right)^{m/p}\right)\mathscr{C}_p(\omega) \pmod{p^{\mathrm{ord}_p(m)}}\\ &\equiv \rho^{\sigma}_{0,m/p}\mathscr{C}_p(\omega) \pmod{p^{\mathrm{ord}_p(m)}}.\end{aligned}$$

The second step uses the obvious fact that the Cartier transform does not change the coefficient of $\frac{dx}{x}$.

In a similar manner one can show that

$$\rho_{1,m}(\omega) \equiv \rho^{\sigma}_{1,m/p}\mathscr{C}^1_p(\omega) (\mathrm{mod}\ p^{\mathrm{ord}_p(m)}).$$

Proposition 4.3 tells us that $\mathscr{C}^1_p(\omega) \equiv \mathscr{C}_p(\omega)(\mathrm{mod}\ pd\widehat{\mathscr{O}}_{f^\sigma})$. Together with the first part of our lemma, which implies that $\rho^{\sigma}_{1,m/p}(pd\widehat{\mathscr{O}}_{f^\sigma}) \equiv 0(\mathrm{mod}\ p^{\mathrm{ord}_p(m)})$, we get

$$\rho_{1,m}(\omega) \equiv \rho^{\sigma}_{1,m/p}\mathscr{C}_p(\omega) (\mathrm{mod}\ p^{\mathrm{ord}_p(m)}).$$

In a similar way the statement for $\rho_{\pm,m}$ follows. □

Corollary 5.5. *Let notations be as in Corollary 5.3 Let $Y_m(t)$ be the matrix $Y(t)$, where the entries have been truncated at t^m. Then, for any $m, s \geq 1$,*

$$Y_{mp^s}(t) \equiv (Y(t)Y(t^p)^{-1})Y_{mp^{s-1}}(t^p)(\mathrm{mod}\ p^s).$$

Proof. We start with the equality (5), which holds true modulo $pd\widehat{\Omega}_f$ according to [1, (14)]. Then apply $\rho^{\sigma}_{0,mp^{s-1}}$ and use $\rho_{0,mp^s} \equiv \rho^{\sigma}_{0,mp^{s-1}} \circ \mathscr{C}_p(\mathrm{mod}\ p^s)$ to obtain

$$\begin{pmatrix}\rho_{0,mp^s}(dx/f)\\ \rho_{0,mp^s}(xdx/f)\end{pmatrix} \equiv \Lambda_p \begin{pmatrix}\rho^{\sigma}_{0,mp^{s-1}}(dx/f^\sigma)\\ \rho^{\sigma}_{0,mp^{s-1}}(xdx/f^\sigma)\end{pmatrix} (\mathrm{mod}\ p^s).$$

Similarly we obtain

$$\begin{pmatrix}\rho_{\pm,mp^s}(dx/f)\\ \rho_{\pm,mp^s}(xdx/f)\end{pmatrix} \equiv \Lambda_p \begin{pmatrix}\rho^{\sigma}_{\pm,mp^{s-1}}(dx/f^\sigma)\\ \rho^{\sigma}_{\pm,mp^{s-1}}(xdx/f^\sigma)\end{pmatrix} (\mathrm{mod}\ p^s).$$

Our corollary follows from the above evaluations of the mod m periods and $\Lambda_p = Y(t)Y(t^p)^{-1}$. □

We end with the proof of our main theorem.

Proof of Theorem 5.1. The proof follows the same steps as Corollary 5.3, but with the polynomial $f = x^3 - x - 2t/3\sqrt{3}$. This polynomial is defined over $\mathbb{Z}_p[\sqrt{3}][\![t]\!]$ with Frobenius lift σ such that $\sigma(t) = t^p$ and $\sigma(\sqrt{3}) = \epsilon_p\sqrt{3}$. Hence $f^\sigma = x^3 - x - 2\epsilon_p t^p/\sqrt{3}$. We also use the new basis dx/f, $\sqrt{3}x dx/f$ and replace $\rho_\pm$ by $\frac{1}{\sqrt{3}}\rho_\pm$. The adapted version of Corollary 5.3 would then become

$$\Lambda_p = \mathscr{Y}(t) \begin{pmatrix} \epsilon_p & 0 \\ 0 & 1 \end{pmatrix} \mathscr{Y}(t^p)^{-1}.$$

The remainder of the proof follows the same lines as above. □

We finally give, without proof, the system of differential equations for $\mathscr{Y}(t)$ and its congruence version. Again the proof follows the same lines as in [2].

Theorem 5.6. *We have*

$$\frac{d}{dt}\mathscr{Y}(t) = \frac{1}{3(1-t^2)} \begin{pmatrix} 2t & -1 \\ -2 & t \end{pmatrix} \mathscr{Y}(t)$$

and

$$\frac{d}{dt}\mathscr{Y}_{mp^s}(t) \equiv \frac{1}{3(1-t^2)} \begin{pmatrix} 2t & -1 \\ -2 & t \end{pmatrix} \mathscr{Y}_{mp^s}(t) (\mathrm{mod}\ p^s)$$

For all $m, s \geq 1$.

Acknowledgements I would like to thank Ling Long for our discussions which gave rise to this paper. I also like to thank the referees for their valuable feedback and their corrections.

References

1. F. Beukers, M. Vlasenko, *Dwork crystals I*, Int. Math. Res. Notices 2021, 8807–8844, https://doi.org/10.1093/imrn/rnaa119
2. F. Beukers, M. Vlasenko, *Dwork crystals II*, Int. Math. Res. Notices 2021, 4427–4444, https://doi.org/10.1093/imrn/rnaa120
3. B. Dwork, *p-adic cycles*, Publications Mathématiques de l'I.H.É.S. 37 (1969), 27–115
4. N. Katz, *Internal reconstruction of unit-root F-crystals via expansion coefficients. With an appendix by Luc Illusie* Annales scientifiques de l'É.N.S 18 (1985), 245–285
5. A. Mellit, M. Vlasenko, *Dwork's congruences for the constant terms of powers of a Laurent polynomial*, Int. J. Number Theory 12 (2016), 313–321