A METHOD FOR DETERMINING THE MOD-p^k BEHAVIOUR OF RECURSIVE SEQUENCES

C. KRATTENTHALER† AND T. W. MÜLLER*

Abstract. We present a method for obtaining congruences modulo powers of a prime number p for combinatorial sequences whose generating function satisfies an algebraic differential equation. This method generalises the one by Kauers and the authors [*Electron. J. Combin.* **18**(2) (2012), Art. P37] from $p = 2$ to arbitrary primes. Our applications include congruences for numbers of non-crossing graphs and numbers of Kreweras walks modulo powers of 3, as well as congruences for Fuß–Catalan numbers and blossom tree numbers modulo powers of arbitrary primes.

1. Introduction

The purpose of the present article is to generalise the basic theory concerning congruences for combinatorial sequences developed in [12] for 2-power moduli to arbitrary prime power moduli, and to discuss a number of further applications of our method.

Given a prime number p, consider the (formal) power series

$$\Phi(z) = \Phi_p(z) := \sum_{n\ge0} z^{p^n}. \tag{1.1}$$

The series $\Phi_p(z)$ is easily seen to be transcendental over $\mathbb{Z}$; this can be shown, for instance, by generalising (in a straightforward manner) the density argument given in [12, Lemma 1]. In Lemma 1 below, we provide a different, and more elegant, argument, which however presupposes a number of non-trivial facts concerning certain auxiliary series $H_{b_1,b_2,\dots,b_r}(z)$ established in Section 3.

While $\Phi_p(z)$ is transcendental over $\mathbb{Z}$, it is easily seen to be algebraic when considered over finite rings $\mathbb{Z}/p^\gamma\mathbb{Z}$, and the first focus of our paper is on polynomial identities for $\Phi_p(z)$ modulo a given p-power, which are of *minimal degree*; cf. the next section. A (still stubbornly unproven) conjecture concerns this minimal degree of $\Phi_p(z)$ modulo p^γ, see Conjecture 4 in the next section. As in [12, Sec. 2] for the case of the prime $p = 2$, we are only able to establish that the conjectured minimal degree constitutes a lower bound, see Lemma 1.

The basic idea of our method for producing and establishing congruences modulo p-powers for combinatorial sequences is to express solutions of appropriate (formal) differential equations (in technical terms: differentially algebraic power series over the integers satisfying a uniqueness condition) as *polynomials in* $\Phi_p(z)$, *with coefficients*

2010 *Mathematics Subject Classification.* Primary 05A15; Secondary 05E99 11A07 68W30.

Key words and phrases. Polynomial recurrences, Fuß–Catalan numbers, non-crossing graphs, Kreweras walks, blossom trees.

†Research partially supported by the Austrian Science Foundation FWF, grants Z130-N13 and F50-N15, the latter in the framework of the Special Research Program "Algorithmic and Enumerative Combinatorics".

*Research supported by Lise Meitner Grant M1661-N25 of the Austrian Science Foundation FWF.

that are Laurent polynomials in z. For each such differential equation, our method may be implemented to (semi-)automatically yield such polynomial expressions in $\Phi_p(z)$ for arbitrary p-power moduli, provided such expressions do in fact exist.

However, such a procedure as described in the last paragraph would be without any practical value, if we could not, at the same time, provide an efficient algorithm for *extracting coefficients from powers of* $\Phi_p(z)$. This is the topic of Section 3. Briefly, the solution to this problem we propose is to (i) *expand powers of* $\Phi_p(z)$ into $\mathbb{Z}$-linear sums of certain auxiliary series

$$H_{b_1,b_2,\dots,b_r}(z) := \sum_{n_1>n_2>\dots>n_r\ge 0} z^{b_1p^{n_1}+b_2p^{n_2}+\dots+b_rp^{n_r}}; \tag{1.2}$$

(ii) to show that the set consisting of 1 and the series (1.2) with parameters $b_1, b_2, \dots, b_r$ relatively prime to p are *linearly independent over the ring* $\mathbb{Z}[z, z^{-1}]$*, as well as over the rings* $(\mathbb{Z}/p^\gamma\mathbb{Z})[z, z^{-1}]$; (iii) to prove that a series $H_{b_1,b_2,\dots,b_r}(z)$, without restrictions on its parameters $b_1, b_2, \dots, b_r$, can always *be expressed as a linear combination over* $\mathbb{Z}[z, z^{-1}]$ of these linear independent series; and (iv) to demonstrate that *coefficient extraction from a series* (1.2) *with all parameters* $b_1, b_2, \dots, b_r$ *relatively prime to* p *can be done effectively*; cf. Equation (3.1), Corollary 7, Proposition 9, and Remark 8.

A detailed description of our method is given in Section 4, while the remaining sections treat a number of applications beyond the case where $p = 2$: in Section 5, we obtain congruences modulo arbitrary 3-powers for the number of non-crossing graphs with a given number of vertices; Section 6 deals with congruences modulo 3-powers for the number of Kreweras walks of given length in the plane; Section 7 treats the Fuß–Catalan numbers

$$F(n;k) := \frac{1}{n}\binom{kn}{n-1}$$

modulo powers of a prime number p, provided that the parameter k is itself a power of p; finally, the last section studies the number

$$B(n;p) := \frac{p+1}{n((p-1)n+2)}\binom{pn}{n-1}$$

of p-ary blossom trees with n white nodes modulo arbitrary powers of p. See, in particular, Theorems 11, 12, 15, 16, 19, 20, 23, and 25.

We would like to point out that Rowland and Yassawi [17] have developed a completely different method for proving congruences. Their method applies to diagonals of rational functions, and is based on the construction of automata. Our method is complementary: there is a considerable intersection of applications (in particular, if one also adds the variation [13] of the method presented here), but neither can our method cover all diagonals of rational functions nor can their method cover all differentially algebraic series. Applications of our method not covered by [17] can be found in [12, Sections 8–14].

2. The p-power series $\Phi_p(z)$

The series $\Phi_p(z)$ in (1.1) is the principal character in the method for determining congruences of recursive sequences modulo p-powers which we describe in Section 4. For the sake of better readability, we shall usually suppress the index p and simply write $\Phi(z)$ for $\Phi_p(z)$. It is not hard to see that this series is transcendental over $\mathbb{Z}[z]$ (this follows for instance from Lemma 1 below). However, if the coefficients of $\Phi(z)$ are considered modulo a p-power p^γ, then $\Phi(z)$ obeys a polynomial relation with coefficients that are polynomials in z. The focus of this section is on what may be said concerning such polynomial relations, and, in particular, about those of minimal length. In the proofs of Lemma 1 and Proposition 2 below, we shall already make use of some fundamental results which will only be established later in Section 3. This will not create any circular arguments since Lemma 1 and Proposition 2 will not be needed in Section 3.

Here and in the sequel, given power series (or Laurent series) $f(z)$ and $g(z)$, we write

$$f(z) = g(z) \text{ modulo } p^\gamma$$

to mean that the coefficients of z^i in $f(z)$ and $g(z)$ agree modulo p^γ for all i.

We say that a polynomial $A(z,t)$ in z and t is *minimal for the modulus* p^γ, if it is monic (as a polynomial in t), has integral coefficients, satisfies $A(z,\Phi(z)) = 0$ modulo p^γ, and there is no monic polynomial $B(z,t)$ with integral coefficients of t-degree less than that of $A(z,t)$ with $B(z,\Phi(z)) = 0$ modulo p^γ. (Minimal polynomials are not unique; see Remark 3.) Furthermore, we let $v_p(\alpha)$ denote the p-adic valuation of the integer α, that is, the maximal exponent e such that p^e divides α.

The lemma below provides a lower bound for the degree of a polynomial that is minimal for the modulus p^γ.

Lemma 1. *If $A(z,t)$ is minimal for the modulus p^γ, then the degree d of $A(z,t)$ in t satisfies $v_p(d!) \ge \gamma$. In particular, the series $\Phi(z)$ is transcendental over $\mathbb{Z}[z]$.*

Proof. Given positive integers $b_1, b_2, \dots, b_r$, define the series $H_{b_1,b_2,\dots,b_r}(z)$ by

$$H_{b_1,b_2,\dots,b_r}(z) := \sum_{n_1>n_2>\dots>n_r\ge 0} z^{b_1p^{n_1}+b_2p^{n_2}+\dots+b_rp^{n_r}}.$$

By (3.1) and Proposition 9, a power $\Phi^d(z)$ can be expressed as a linear combination of series $H_{b_1,b_2,\dots,b_s}(z)$ and 1 with coefficients in $\mathbb{Z}[z]$. Furthermore, all b_i's in these series are relatively prime to p, and $b_1 + b_2 + \dots + b_s \le d$. In particular, we have

$$\Phi^d(z) = d!\, H_{1,1,\dots,1}(z) + \text{other terms}, \tag{2.1}$$

with d repetitions of 1 in the index of H. Since, by Corollary 7, the series $H_{b_1,b_2,\dots,b_s}(z)$ and 1 are linearly independent over $(\mathbb{Z}/p^\gamma\mathbb{Z})[z]$, and $H_{1,1,\dots,1}(z)$ (with d repetitions of 1) does not appear in the expansion of $\Phi^e(z)$ for $e < d$, a monic polynomial of degree d in $\Phi(z)$ can only vanish modulo p^γ if $d! \equiv 0 \pmod{p^\gamma}$, or, equivalently, if $v_p(d!) \ge \gamma$. This establishes the assertion. □

Proposition 2. *Minimal polynomials for the moduli $p, p^2, p^3, \dots, p^{p+1}$ are*

$$\begin{aligned}
&t^p - t + z && \text{modulo } p,\\
&(t^p - t + z)^2 && \text{modulo } p^2,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\\
&(t^p - t + z)^p && \text{modulo } p^p,\\
&(t^p - t + z)^p - p^{p-1}(t^2 - t + z) && \text{modulo } p^{p+1},
\end{aligned}$$

Proof. By (3.1), we have

$$\Phi^p(z) = \sum_{r=1}^{p} \sum_{\substack{b_1,\dots,b_r\ge1\\ b_1+\dots+b_r=p}} \frac{p!}{b_1!\,b_2!\cdots b_r!} H_{b_1,b_2,\dots,b_r}(z)$$
$$= \sum_{n\ge0} z^{p^{n+1}} + p \sum_{r=2}^{p} \sum_{\substack{b_1,\dots,b_r\ge1\\ b_1+\dots+b_r=p}} \frac{(p-1)!}{b_1!\,b_2!\cdots b_r!} H_{b_1,b_2,\dots,b_r}(z),$$

or, equivalently,

$$\Phi^p(z) - \Phi(z) + z = p \sum_{r=2}^{p} \sum_{\substack{b_1,\dots,b_r\ge1\\ b_1+\dots+b_r=p}} \frac{(p-1)!}{b_1!\,b_2!\cdots b_r!} H_{b_1,b_2,\dots,b_r}(z). \tag{2.2}$$

Clearly, this implies the claim modulo p, and, by potentiation, as well the claims modulo p^i for $i = 2, 3, \dots, p$.

Taking both sides of (2.2) to the p-th power, we obtain

$$(\Phi^p(z) - \Phi(z) + z)^p = p^p \sum_{r=2}^{p} \sum_{\substack{b_1,\dots,b_r\ge1\\ b_1+\dots+b_r=p}} \left(\frac{(p-1)!}{b_1!\,b_2!\cdots b_r!}\right)^p H^p_{b_1,b_2,\dots,b_r}(z) + O\left(p^{p+1}\right),$$

where the expression $O\left(p^{p+1}\right)$ subsumes terms all of whose coefficients are divisible by p^{p+1}. If, in the sum over r on the right-hand side, we use the congruences $N^p \equiv N \pmod p$, which is valid for any integer N, and

$$H^p_{b_1,b_2,\dots,b_r}(z) = H_{b_1,b_2,\dots,b_r}(z) + O\left(p\right),$$

then, in combination with (2.2) read from right to left, we obtain the claim on the minimal polynomial modulo p^{p+1}. ☐

Remark 3. Minimal polynomials are highly non-unique: for example, the polynomial

$$(t^p - t + z)^2 + p(t^p - t + z)$$

is obviously also a minimal polynomial for the modulus p^2.

Based on the observations in Proposition 2 and Lemma 1, we propose the following conjecture.

Conjecture 4. *The degree of a minimal polynomial for the modulus p^γ, $\gamma \ge 1$, is the least d such that $v_p(d!) \ge \gamma$.*

Remark 5. (1) Given the p-ary expansion of d, say

$$d = d_0 + d_1 \cdot p + d_2 \cdot p^2 + \dots + d_r \cdot p^r, \quad 0 \le d_i \le p-1,$$

by the well-known formula of Legendre [15, p. 10], we have

$$v_p(d!) = \sum_{\ell=1}^{\infty} \left\lfloor \frac{d}{p^\ell} \right\rfloor = \sum_{\ell=1}^{\infty} \left\lfloor \sum_{i=0}^{r} d_i p^{i-\ell} \right\rfloor = \sum_{\ell=1}^{\infty} \sum_{i=\ell}^{r} d_i p^{i-\ell}$$
$$= \sum_{i=1}^{r} \sum_{\ell=1}^{i} d_i p^{i-\ell} = \sum_{i=1}^{r} d_i \frac{p^i - 1}{p-1} = \frac{d - s(d)}{p-1}, \tag{2.3}$$

where $s(d)$ denotes the sum of digits of d in its p-ary expansion. Consequently, an equivalent way of phrasing Conjecture 4 is to say that the degree of a minimal polynomial for the modulus p^γ is the least d with $d - s(d) \ge (p-1)\gamma$.

(2) We claim that, in order to establish Conjecture 4, it suffices to prove the conjecture for $\gamma = \frac{p^\delta - 1}{p-1}$, $\delta = 1, 2, \dots$. If we take into account Lemma 1 plus the above remark, this means that it is sufficient to prove that, for each $\delta \ge 1$, there is a polynomial $A_\delta(z,t)$ of degree p^δ such that

$$A_\delta(z, \Phi(z)) = 0 \quad \text{modulo } p^{(p^\delta - 1)/(p-1)}. \tag{2.4}$$

For, arguing by induction, let us suppose that we have already constructed $A_1(z,t)$, $A_2(z,t), \dots, A_m(z,t)$ satisfying (2.4). Let α be a positive integer which is divisible by p and

$$\alpha = \alpha_1 \cdot p + \alpha_2 \cdot p^2 + \cdots + \alpha_m \cdot p^m, \quad 0 \le \alpha_i \le p-1,$$

be its p-ary expansion. Then we have

$$\prod_{\delta=1}^{m} A_\delta^{\alpha_\delta}(z, \Phi(z)) = 0 \quad \text{modulo } \prod_{\delta=1}^{m} p^{\alpha_\delta (p^\delta - 1)/(p-1)} = p^{(\alpha - s(\alpha))/(p-1)}. \tag{2.5}$$

On the other hand, the degree of the left-hand side of (2.5) as a polynomial in $\Phi(z)$ is $\sum_{\delta=1}^{m} \alpha_\delta p^\delta = \alpha$.

Let us put these observations together. In view of (2.3), Lemma 1 says that the degree of a minimal polynomial for the modulus p^γ cannot be smaller than the least integer, $d^{(\gamma)}$ say, for which $d^{(\gamma)} - s(d^{(\gamma)}) \ge (p-1)\gamma$. (We point out that $d^{(\gamma)}$ must be automatically divisible by p.) If we take into account that the quantity $\alpha - s(\alpha)$, as a function in α, is weakly monotone increasing in α, then (2.5) tells us that, as long as

$$d^{(\gamma)} \le (p-1)p + (p-1)p^2 + \cdots + (p-1)p^m = p^{m+1} - p,$$

we have found a monic polynomial of degree $d^{(\gamma)}$, $B_\gamma(z,t)$ say, for which $B_\gamma(z, \Phi(z)) = 0$ modulo p^γ, namely the left-hand side of (2.5) with α replaced by $d^{(\gamma)}$, to wit

$$B_\gamma(z,t) = \prod_{\delta=1}^{m} A_\delta^{d_\delta^{(\gamma)}}(z,t),$$

where $d^{(\gamma)} = d_1^{(\gamma)} \cdot p + d_2^{(\gamma)} \cdot p^2 + \cdots + d_m^{(\gamma)} \cdot p^m$ is the p-ary expansion of $d^{(\gamma)}$. Hence, it must necessarily be a minimal polynomial for the modulus p^γ.

Since

$$p^{m+1} - p - s(p^{m+1} - p) = p^{m+1} - p - (p-1)m,$$

we have thus found minimal polynomials for all moduli p^γ with $\gamma \le \frac{p^{m+1}-p}{p-1} - m$. Now we should note that the quantity $\alpha - s(\alpha)$ makes a jump from $p^{m+1} - p - (p-1)m$ to $p^{m+1} - 1$ when we move from $\alpha = p^{m+1} - p$ to $\alpha = p^{m+1}$ (the reader should recall that it suffices to consider α's which are divisible by p). If we take $A_m^p(z,t)$, which has degree $p \cdot p^m = p^{m+1}$, then, by (2.4), we also have a minimal polynomial for the modulus

$$\left(p^{(p^m - 1)/(p-1)}\right)^p = p^{(p^{m+1} - p)/(p-1)}$$

and, in view of the preceding remark, as well for all moduli p^γ with γ between $\frac{p^{m+1}-p}{p-1} - m + 1$ and $\frac{p^{m+1}-p}{p-1}$.

So, indeed, the first modulus for which we do not have a minimal polynomial is the modulus $p^{(p^{m+1}-p)/(p-1)+1} = p^{(p^{m+1}-1)/(p-1)}$. This is the role which $A_{m+1}(z,t)$ (see (2.4) with $m+1$ in place of δ) would have to play.

The arguments above show at the same time that, supposing that we have already constructed $A_1(z,t), A_2(z,t), \dots, A_m(z,t)$, the polynomial $A_m^p(z,t)$ is a very close "approximation" to the polynomial $A_{m+1}(z,t)$ that we are actually looking for next, which is only "off" by a factor of p. In practice, one can recursively compute polynomials $A_\delta(z,t)$ satisfying (2.4) by following the procedure outlined in the next-to-last paragraph before Lemma 6 in the next section. It is these computations (part of which are reported in Proposition 2) which have led us to believe in the truth of Conjecture 4.

3. Coefficient extraction from powers of $\Phi(z)$

In the next section we are going to describe a method for expressing formal power series satisfying certain differential equations, after the coefficients of the series have been reduced modulo p^k, as polynomials in the p-power series $\Phi(z)$ (which has been discussed in the previous section; for the definition see (1.1)), the coefficients being Laurent polynomials in z. Such a method would be without value if we could not, at the same time, provide a procedure for extracting coefficients from powers of $\Phi(z)$. The description of such a procedure is the topic of this section.

Clearly, a brute force expansion of a power $\Phi^K(z)$, where K is a given positive integer, yields

$$\Phi^K(z) = \sum_{r=1}^{K} \sum_{\substack{b_1,\dots,b_r \ge 1\\ b_1+\dots+b_r=K}} \frac{K!}{b_1!\, b_2! \cdots b_r!} H_{b_1,b_2,\dots,b_r}(z), \tag{3.1}$$

where

$$H_{b_1,b_2,\dots,b_r}(z) := \sum_{n_1>n_2>\dots>n_r\ge 0} z^{b_1p^{n_1}+b_2p^{n_2}+\dots+b_rp^{n_r}}.$$

The expansion (3.1) is not (yet) suited for our purpose, since, when $b_1, b_2, \dots, b_r$ vary over all possible choices such that their sum is K, the series $H_{b_1,b_2,\dots,b_r}(z)$ are *not* linearly independent over the ring $\mathbb{Z}[z,z^{-1}]$ of Laurent polynomials in z over the integers[1], and, secondly, coefficient extraction from a series $H_{b_1,b_2,\dots,b_r}(z)$ can be a hairy task if some of the b_i's are divisible by p.

However, we shall show (see Corollary 7) that, if we restrict to b_i's which are *relatively prime to* p, then the corresponding series $H_{b_1,b_2,\dots,b_r}(z)$, together with the (trivial) series 1, *are* linearly independent over $\mathbb{Z}[z,z^{-1}]$, and there is an efficient algorithm to express an arbitrary series $H_{b_1,b_2,\dots,b_s}(z)$, without any restriction on the b_i's, as a linear combination over $\mathbb{Z}[z,z^{-1}]$ of 1 and the former series (see Proposition 9). Since coefficient extraction from a series $H_{b_1,b_2,\dots,b_r}(z)$ with all b_i's relatively prime to p is straightforward (see Remark 8), this solves the problem of coefficient extraction from powers of $\Phi(z)$.

As a side result, the procedure which we described in the previous paragraph, and which will be substantiated below, in combination with (3.1), provides all the means for determining minimal polynomials in the sense of Section 2: as explained in Item (2) of Remark 5 at the end of that section, it suffices to find a minimal polynomial for the

[1]The same is true for an arbitrary commutative unital ring in place of the ring $\mathbb{Z}$ of integers.

modulus $p^{(p^\delta-1)/(p-1)}$, $\delta=1,2,\dots$. For doing this, we would take a minimal polynomial $A_{\delta-1}(z,t)$ for the modulus $p^{(p^{\delta-1}-1)/(p-1)}$, expand $A_{\delta-1}^p(z,t)$, and replace each coefficient $c_{\alpha,\beta}$ of a monomial $z^\alpha t^\beta$ in $A_{\delta-1}^p(z,t)$ by $c_{\alpha,\beta}+p^{(p^\delta-p)/(p-1)}x_{\alpha,\beta}$, where $x_{\alpha,\beta}$ is a variable, thereby obtaining a modified polynomial, $B_{\delta-1}(z,t)$ say. Now we would substitute $\Phi(z)$ for t, so that we obtain $B_{\delta-1}(z,\Phi(z))$. Here, we express powers of $\Phi(z)$ in terms of the series $H_{a_1,a_2,\dots,a_r}(z)$ with all a_i's relatively prime to p, and collect terms. By reading the coefficients of $z^\gamma H_{a_1,a_2,\dots,a_r}(z)$ in this expansion of $B_{\delta-1}(z,\Phi(z))$ and equating them to zero modulo $p^{(p^\delta-1)/(p-1)}$, we produce a system of linear equations modulo $p^{(p^\delta-1)/(p-1)}$ in the unknowns $x_{\alpha,\beta}$. By the definition of $A_{\delta-1}(z,t)$, after division by $p^{(p^\delta-p)/(p-1)}$, this system reduces to a system modulo p, that is, to a linear system of equations over the field with p elements. A priori, this system need not have a solution, but experience seems to indicate that it always does; see Conjecture 4.

We start with an auxiliary result pertaining to the uniqueness of representations of integers as sums of powers of p with multiplicities, tailor-made for application to the series $H_{a_1,a_2,\dots,a_r}(z)$.

Lemma 6. *Let d,r,s be positive integers with $r\ge s$, c an integer with $|c|\le d$, and let $a_1,a_2,\dots,a_r$ respectively $b_1,b_2,\dots,b_s$ be two sequences of integers, none of the a_i's or b_i's divisible by p, with $1\le a_i\le d$ for $1\le i\le r$, and $1\le b_i\le d$ for $1\le i\le s$. If*

$$a_1p^{2rd}+a_2p^{2(r-1)d}+\cdots+a_rp^{2d}=b_1p^{n_1}+b_2p^{n_2}+\cdots+b_sp^{n_s}+c \tag{3.2}$$

for integers $n_1,n_2,\dots,n_s$ with $n_1>n_2>\cdots>n_s\ge 0$, then $r=s$, $c=0$, $a_i=b_i$, and $n_i=2d(r+1-i)$ for $i=1,2,\dots,r$.

Proof. We use induction on r.

First, let $r=1$. Then $s=1$ as well, and (3.2) becomes

$$a_1p^{2d}=b_1p^{n_1}+c. \tag{3.3}$$

If $n_1>2d$, then the above equation implies

$$a_1p^{2d}\equiv c \quad \text{modulo } p^{2d+1}. \tag{3.4}$$

Consequently, the integer c must be divisible by p^{2d}. By assumption, we have $|c|\le d$. Since $d<p^{2d}$, the only possibility is that c vanishes. But then it follows from (3.4) that a_1 is divisible by p, a contradiction.

If $d<n_1<2d$, then it follows from (3.3) that c must be divisible by p^{n_1}. Again by assumption, we have $|c|\le d<p^d<p^{n_1}$, so that $c=0$. But then (3.3) cannot be satisfied since b_1 is assumed not to be divisible by p.

If $0\le n_1\le d$, then we estimate

$$b_1p^{n_1}+c\le d\left(p^d+1\right)\le(p^d-1)(p^d+1)<p^{2d},$$

which is again a contradiction to (3.3).

The only remaining possibility is $n_1=2d$. If this is substituted in (3.3) and the resulting equation is combined with $|c|\le d<p^{2d}$, then the conclusion is that the equation can only be satisfied if $c=0$ and $a_1=b_1$, in accordance with the assertion of the lemma.

We now perform the induction step. We assume that the assertion of the lemma is established for all $r<R$, and we want to show that this implies its validity for $r=R$.

Let t be maximal such that $n_t \ge 2d$. Then reduction of (3.2) modulo p^{2d} yields

$$b_{t+1}p^{n_{t+1}} + b_{t+2}p^{n_{t+2}} + \dots + b_s p^{n_s} + c \equiv 0 \quad \text{modulo } p^{2d}. \tag{3.5}$$

Let us write $b \cdot p^{2d}$ for the left-hand side in (3.5). Then, by dividing (3.2) (with R instead of r) by p^{2d}, we obtain

$$a_1 p^{2(R-1)d} + a_2 p^{2(R-2)d} + \dots + a_{R-1}p^{2d} = b_1 p^{n_1-2d} + b_2 p^{n_2-2d} + \dots + b_t p^{n_t-2d} + b - a_R. \tag{3.6}$$

We have

$$0 \le b \le p^{-2d} d \left(p^{2d-1} + p^{2d-2} + \dots + p^{2d-s+t} + 1\right) \\ \le p^{-2d} d \left(\tfrac{1}{p-1}(p^{2d} - p^{2d-s+t}) + 1\right) \le d.$$

Consequently, we also have $|b - a_R| \le d$. This means that we are in a position to apply the induction hypothesis to (3.6). The conclusion is that $t = R-1$, $b - a_R = 0$, $a_i = b_i$, and $n_i = 2d(R+1-i)$ for $i = 1, 2, \dots, R-1$. If this is used in (3.2) with $r = R$, then we obtain

$$a_R p^{2d} = c$$

or

$$a_R p^{2d} = b_R p^{n_R} + c,$$

depending on whether $s = R-1$ or $s = R$. The first case is absurd, since $c \le d < p^{2d} \le a_R p^{2d}$. On the other hand, the second case has already been considered in (3.3), and we have seen there that it follows that $c = 0$, $a_R = b_R$, and $n_R = 2d$.

This completes the proof of the lemma. $\square$

The announced independence of the series $H_{a_1,a_2,\dots,a_r}(z)$ with all a_i's relatively prime to p is now an easy consequence.

Corollary 7. *For any commutative unital ring R, the series $H_{a_1,a_2,\dots,a_r}(z)$, with all a_i's relatively prime to p, together with the series 1 are linearly independent over $R[z, z^{-1}]$. In particular, they are linearly independent over $(\mathbb{Z}/p\mathbb{Z})[z, z^{-1}]$, over $(\mathbb{Z}/p^\gamma\mathbb{Z})[z, z^{-1}]$ for an arbitrary positive integer γ, and over $\mathbb{Z}[z, z^{-1}]$.*

Proof. Let us suppose that

$$q_0(z) + \sum_{i=1}^{N} q_i(z) H_{a_1^{(i)}, a_2^{(i)}, \dots, a_{r_i}^{(i)}}(z) = 0, \tag{3.7}$$

where the $q_i(z)$'s are non-zero Laurent polynomials in z over R, the r_i's are positive integers, and $a_j^{(i)}$, $j = 1, 2, \dots, r_i$, $i = 1, 2, \dots, N$, are integers relatively prime to p. We may also assume that the tuples $(a_1^{(i)}, a_2^{(i)}, \dots, a_{r_i}^{(i)})$, $i = 1, 2, \dots, N$, are pairwise distinct. Choose i_0 such that r_{i_0} is maximal among the r_i's. Without loss of generality, we may assume that the coefficient of z^0 in $q_{i_0}(z)$ is non-zero (otherwise we could multiply both sides of (3.7) by an appropriate power of z). Let d be the maximum of all $a_j^{(i)}$'s and the absolute values of exponents of z appearing in monomials with non-zero coefficient in the Laurent polynomials $q_i(z)$, $i = 0, 1, \dots, N$. Then, according to Lemma 6 with $r = r_{i_0}$, $a_j = a_j^{(i_0)}$, $j = 1, 2, \dots, r_{i_0}$, the coefficient of

$$z^{a_1^{(i_0)} p^{2rd} + a_2^{(i_0)} p^{2(r-1)d} + \dots + a_r^{(i_0)} p^{2d}}$$

is 1 in $H_{a_1^{(i_0)},a_2^{(i_0)},\dots,a_{r_{i_0}}^{(i_0)}}(z)$, while it is zero in series $z^e H_{a_1^{(i_0)},a_2^{(i_0)},\dots,a_{r_{i_0}}^{(i_0)}}(z)$, where e is a non-zero integer with $|e| \le d$, and in all other series $z^e H_{a_1^{(i)},a_2^{(i)},\dots,a_{r_i}^{(i)}}(z)$, $i = 1, \dots, i_0 - 1, i_0 + 1, \dots, N$, where e is a (not necessarily non-zero) integer with $|e| \le d$. This contradiction to (3.7) establishes the assertion of the corollary. □

Remark 8. Coefficient extraction from a series $H_{a_1,a_2,\dots,a_r}(z)$ with all a_i's relatively prime to p is straightforward: if we want to know whether z^M appears in $H_{a_1,a_2,\dots,a_r}(z)$, that is, whether we can represent M as

$$M = a_1 p^{n_1} + a_2 p^{n_2} + \cdots + a_r p^{n_r}$$

for some $n_1, n_2, \dots, n_r$ with $n_1 > n_2 > \cdots > n_r \ge 0$, then necessarily $n_r = v_p(M)$, $n_{r-1} = v_p(M - a_r p^{n_r})$, etc. The term z^M appears in $H_{a_1,a_2,\dots,a_r}(z)$ if, and only if, the above process terminates after *exactly* r steps. This means, that, with $n_r, n_{r-1}, \dots, n_1$ constructed as above, we have

$$M - (a_s p^{n_s} + \cdots + a_{r-1} p^{n_{r-1}} + a_r p^{n_r}) > 0$$

for $s > 1$, and

$$M - (a_1 p^{n_1} + \cdots + a_{r-1} p^{n_{r-1}} + a_r p^{n_r}) = 0.$$

It should be noted that, given $a_1, a_2, \dots, a_r$, this procedure of coefficient extraction needs at most $O(\log M)$ operations, that is, its computational complexity is linear.

It remains to show that an arbitrary series $H_{b_1,b_2,\dots,b_s}(z)$ can be expressed as a linear combination over $\mathbb{Z}[z, z^{-1}]$ of the series 1 and the series $H_{a_1,a_2,\dots,a_r}(z)$, where all a_i's are relatively prime to p.

Proposition 9. *For any positive integers $b_1, b_2, \dots, b_r$, the series $H_{b_1,b_2,\dots,b_s}(z)$ can be expressed as a linear combination over $\mathbb{Z}[z]$ of the series 1 and series of the form $H_{a_1,a_2,\dots,a_s}(z)$, where all a_i's are relatively prime to p, $s \le r$, and $a_1 + a_2 + \cdots + a_s \le b_1 + b_2 + \cdots + b_r$.*

Proof. Given $H_{b_1,b_2,\dots,b_s}(z)$ where not all b_i's are relatively prime to p, we let h be maximal such that $b_h \equiv 0 \pmod p$. If there is no such h, then there is nothing to do. If there is, then we apply the appropriate case of

$$\begin{aligned} &H_{b_1,\dots,b_{h-1},pb'_h,b_{h+1},\dots,b_r}(z) \\ &\quad = \begin{cases} H_{b_1,\dots,b_{h-1},b'_h,b_{h+1},\dots,b_r}(z) + H_{b_1,\dots,b_{h-1}+b'_h,b_{h+1},\dots,b_r}(z) - H_{b_1,\dots,b_{h-1},pb'_h+b_{h+1},\dots,b_r}(z), \\ \hfill \text{if } 1 < h < r, \\ H_{b'_1,b_2,\dots,b_r}(z) - H_{pb'_1+b_2,\dots,b_r}(z), & \text{if } 1 = h < r, \\ H_{b_1,\dots,b_{h-1},b'_h}(z) + H_{b_1,\dots,b_{h-1}+b'_h}(z) - z^{b'_h} H_{b_1,\dots,b_{h-1}}(z), & \text{if } 1 < h = r, \\ H_{b'_1}(z) - z^{b'_1}, & \text{if } 1 = h = r. \end{cases} \end{aligned} \tag{3.8}$$

These identities are due to Hou [11], and they are straightforward to verify. The reduction (3.8) is now applied to the series which arose during the first application of (3.8). This process is repeated until all series $H_{a_1,a_2,\dots,a_s}(z)$ in the obtained expression have the property that each index a_i is relatively prime to p. From (3.8), it is obvious that all these series satisfy $a_1 + a_2 + \cdots + a_s \le b_1 + b_2 + \cdots + b_r$. This proves the assertions of the proposition. □

To conclude this section, let us provide an illustration of the above discussion. We set ourselves the task of determining the coefficient of $z^{297398301914493}$ in $\Phi^5(z)$ for $\Phi(z) = \sum_{n\ge0} z^{3^n}$. In order to accomplish this task, we first express $\Phi^5(z)$ in terms of series $H_{a_1,\dots,a_r}(z)$ with all a_i's being relatively prime to 3. Indeed, by means of the expansion (3.1) and the algorithm described in the proof of Proposition 9, we have

$$\begin{multline} \Phi^5(z) = 120H_{1,1,1,1,1}(z) + 60H_{2,1,1,1}(z) + 60H_{1,2,1,1}(z) + 60H_{1,1,2,1}(z) + 60H_{1,1,1,2}(z)\\ + 30H_{2,2,1}(z) + 30H_{2,1,2}(z) + 30H_{1,2,2}(z) - 15H_{4,1}(z) - 15H_{1,4}(z) - 9H_5(z)\\ + 60H_{1,1,1}(z) + 30H_{2,1}(z) + 30H_{1,2}(z) - 20zH_{1,1}(z) - 10zH_2(z) + 10H_1(z) - 10z. \end{multline} \tag{3.9}$$

Now we have to answer the question, in which of the series $H_{a_1,\dots,a_r}(z)$ that appear in this expansion of $\Phi^5(z)$ do we find the monomial $z^{297398301914493}$. Using the algorithm described in Remark 8, we see that

$$\begin{aligned} 297398301914493 &= 3^{30} + 3^{29} + 3^{28},\\ &= 2\cdot 3^{29} + 2\cdot 3^{29} + 3^{28},\\ &= 2\cdot 3^{28} + 3^{28} + 2\cdot 3^{28} + 183014339639688,\\ &= 3^{30} + 2\cdot 3^{28} + 2\cdot 3^{28},\\ &= 4\cdot 3^{29} + 3^{28},\\ &= 3^{30} + 4\cdot 3^{28},\\ &= 3^{29} + 3^{29} + 2\cdot 3^{29} + 3^{28},\\ &= 3^{30} + 3^{28} + 3^{28} + 2\cdot 328,\\ &= 5\cdot 3^{28} + 183014339639688,\\ &= 2\cdot 3^{29} + 3^{28} + 137260754729766,\\ &= 3^{28} + 2\cdot 28 + 228767924549610,\\ &= 2\cdot 3^{28} + 251644717004571,\\ &= 3^{28} + 274521509459532. \end{aligned}$$

Here, the first line shows that $z^{297398301914493}$ appears in $H_{1,1,1}(z)$ (thereby making it impossible to appear in $H_{1,1,1,1,1}(z)$, $H_{2,1,1,1}(z)$, or $H_{1,2,1,1}(z)$), the fifth line shows that it appears in $H_{4,1}(z)$, and the sixth line shows that it appears in $H_{4,1}(z)$, while the remaining lines show that it does not appear in any other term in the expansion of $\Phi^5(z)$ displayed in (3.9). Hence, by taking into account the coefficients with which the series $H_{1,1,1}(z)$, $H_{4,1}(z)$, and $H_{1,4}(z)$ appear in this expansion, the coefficient of $z^{297398301914493}$ in $\Phi^5(z)$ is seen to equal $60 - 15 - 15 = 30$.

4. The method

We consider a (formal) differential equation

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0, \tag{4.1}$$

where $\mathcal{P}$ is a polynomial with integer coefficients, which has a power series solution $F(z)$ with integer coefficients. We assume that this power series solution $F(z)$ is uniquely determined by (4.1) over the integers, and also over all rings $(\mathbb{Z}/p^\gamma\mathbb{Z})$, where p is a fixed prime number and γ any positive integer.

In the above situation, we propose the following algorithmic approach to determining the series $F(z)$ modulo a p-power p^{p^α}, for some non-negative integer α. We make the Ansatz

$$F(z) = \sum_{i=0}^{p^{\alpha+1}-1} a_i(z)\Phi^i(z) \quad \text{modulo } p^{p^\alpha}, \tag{4.2}$$

with $\Phi(z)$ as given in (1.1), and where the $a_i(z)$'s are (at this point) undetermined Laurent polynomials in z. Now we substitute (4.2) into (4.1), and we shall gradually determine approximations $a_{i,\beta}(z)$ to $a_i(z)$ such that (4.1) holds modulo p^β, for $\beta = 1, 2, \dots, p^\alpha$. To start the procedure, we consider the differential equation (4.1) modulo p, with

$$F(z) = F_1(z) = \sum_{i=0}^{p^{\alpha+1}-1} a_{i,1}(z)\Phi^i(z) \quad \text{modulo } p. \tag{4.3}$$

Using the elementary fact that $\Phi'(z) = 1$ modulo p, we see that the left-hand side of (4.1) is a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z. We reduce powers $\Phi^k(z)$ with $k \ge p^{\alpha+1}$ using the relation (which is implied by the minimal polynomial for the modulus p given in Proposition 2) [2]

$$\big(\Phi^p(z) - \Phi(z) + z\big)^{p^\alpha} = 0 \quad \text{modulo } p^{p^\alpha}. \tag{4.4}$$

Since, at this point, we are only interested in finding a solution to (4.1) modulo p, the above relation simplifies to

$$\Phi^{p^{\alpha+1}}(z) - \Phi^{p^\alpha}(z) + z^{p^\alpha} = 0 \quad \text{modulo } p. \tag{4.5}$$

Now we compare coefficients of powers $\Phi^k(z)$, $k = 0, 1, \dots, p^{\alpha+1} - 1$ (see Remark 10). This yields a system of $p^{\alpha+1}$ (differential) equations (modulo p) for the unknown Laurent polynomials $a_{i,1}(z)$, $i = 0, 1, \dots, p^{\alpha+1} - 1$, which may or may not have a solution.

Provided we have already found Laurent polynomials $a_{i,\beta}(z)$, $i = 0, 1, \dots, p^{\alpha+1} - 1$, for some β with $1 \le \beta \le p^\alpha - 1$, such that

$$\sum_{i=0}^{p^{\alpha+1}-1} a_{i,\beta}(z)\Phi^i(z) \tag{4.6}$$

[2] Actually, if we would like to obtain an optimal result, we should use the relation implied by a minimal polynomial for the modulus p^{p^α} in the sense of Section 2. But since we have no general formula available for such a minimal polynomial (cf. Item (2) of Remark 5 in that section), and since we wish to prove results for arbitrary moduli, choosing instead powers of a minimal polynomial for the modulus p is the best compromise. In principle, it may happen that there exists a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z, which is identical with $F(z)$ after reduction of its coefficients modulo p^{p^α}, but the Ansatz (4.2) combined with the reduction (4.4) fails because it is too restrictive. We are not aware of a concrete example where this obstruction occurs. The subgroup numbers of $SL_2(\mathbb{Z})$ which are treated modulo 8 in [12, Section 11] by the method described here (specialised to $p = 2$), and modulo 16 by an enhancement of the method outlined in [12, Appendix D] are a potential candidate when considered modulo 2^β for $\beta \ge 5$. On the other hand, once we are successful using this (potentially problematic) Ansatz, then the result can easily be converted into an optimal one by further reducing the polynomial thus obtained, using the relation implied by a minimal polynomial for the modulus p^{p^α}.

solves (4.1) modulo p^β, we put

$$a_{i,\beta+1}(z) := a_{i,\beta}(z) + p^\beta b_{i,\beta+1}(z), \quad i = 0, 1, \dots, p^{\alpha+1} - 1, \tag{4.7}$$

where the $b_{i,\beta+1}(z)$'s are (at this point) undetermined Laurent polynomials in z. Next we substitute

$$\sum_{i=0}^{p^{\alpha+1}-1} a_{i,\beta+1}(z)\Phi^i(z) \tag{4.8}$$

for $F(z)$ in (4.1). Using the fact that $\Phi'(z) = \sum_{n=0}^{\beta} p^n z^{p^n-1}$ modulo $p^{\beta+1}$, we expand the left-hand side as a polynomial in $\Phi(z)$ (with coefficients being Laurent polynomials in z), we apply again the reduction using relation (4.4), we compare coefficients of powers $\Phi^k(z)$, $k = 0, 1, \dots, p^{\alpha+1} - 1$ (again, see Remark 10), and, as a result, we obtain a system of $p^{\alpha+1}$ (differential) equations (modulo $p^{\beta+1}$) for the unknown Laurent polynomials $b_{i,\beta+1}(z)$, $i = 0, 1, \dots, p^{\alpha+1}-1$, which may or may not have a solution. If we manage to push this procedure through until $\beta = p^\alpha - 1$, then, setting $a_i(z) = a_{i,p^\alpha}(z)$, $i = 0, 1, \dots, p^{\alpha+1} - 1$, the right-hand side of (4.2) is a solution to (4.1) modulo p^{p^α}, as required.

Remark 10. As the reader will have noticed, each comparison of coefficients of powers of $\Phi(z)$ is based on the "hope" that, if a polynomial in $\Phi(z)$ is zero modulo a p-power p^β (as a formal Laurent series), then already all coefficients of powers of $\Phi(z)$ in this polynomial vanish modulo p^β. However, this implication is false in general (see Lemma 39 in [12, Appendix D] for the case of modulus 16). It may thus happen that the method described in this section fails to find a solution modulo p^β to a given differential equation in the form of a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers, while such a solution does in fact exist. As a matter of fact, this situation already occurred earlier in [12, Theorem 28] in the context of the analysis modulo 16 of the subgroup numbers of $SL_2(\mathbb{Z})$. There exists an enhancement of the method, outlined for the case of $p = 2$ in [12, Appendix D], which (at least in principle) allows us to decide whether or not a solution modulo a given power in terms of a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers exists, and, if so, to explicitly find such a solution. Since we do not make use of this enhancement in the present article, we refrain from presenting it here.

It is not difficult to see that performing the iterative step (4.7) amounts to solving a system of linear differential equations in the unknown functions $b_{i,\beta+1}(z)$ modulo p, where all of them are Laurent polynomials in z, and where only derivatives up to order $p-1$ of the $b_{i,\beta+1}(z)$'s occur. Solving such a system is equivalent to solving an ordinary system of linear equations. This equivalence was explained for the case of $p = 2$ in [12, Lemma 12]. Since we do not need the general version of this lemma for arbitrary primes p in the present article, we leave it to the reader to work out the straightforward details.

We remark that the idea of the method that we have described in this section has certainly further potential. For example, the fact that the series $\Phi(z)$ remains invariant under the substitution $z \to z^p$ (or, more generally, under the substitution $z \to z^{p^h}$, where h is some positive integer) — up to a simple additive correction — can be exploited in order to extend the range of applicability of our method to equations where we not only allow differentiation but also this kind of substitution. This idea is actually already used in Section 7, see Theorem 19.

5. The number of non-crossing connected graphs modulo 3-powers

In this section, we apply our method to determining congruences modulo powers of 3 for the numbers of non-crossing connected graphs with a given number of vertices. The origin of this analysis lies in a conjecture of Deutsch and Sagan [5, Conj. 5.18]. See (5.9) and the subsequent paragraph for more information.

A non-crossing graph on n vertices is a graph whose vertices are labelled by $1, 2, \dots, n$, which can be embedded in the plane without crossings of edges in such a manner that the vertices are placed around a circle in clock-wise order. Let N_n denote the number of non-crossing connected graphs with n vertices. It is known from [9, Eq. (16)] that

$$N_n = \frac{2^{2n-1}}{n}\binom{\frac{3}{2}n-2}{n-1} - \frac{2^{2n-2}}{n}\binom{\frac{3}{2}n-\frac{3}{2}}{n-1}. \tag{5.1}$$

Let $N(z) := \sum_{n\ge1} N_n\, z^n$ be the corresponding generating function. According to [6, Eq. (47)] (see also [8, Sec. 2.1]), the generating function $N(z)$ satisfies the polynomial equation

$$N^3(z) + N^2(z) - 3z\, N(z) + 2z^2 = 0. \tag{5.2}$$

It is not difficult to see that (5.2) determines $N(z)$ uniquely as a formal power series over $\mathbb{Z}$, and as well modulo any power of 3, provided $N_0 = 0$ and $N_1 = 1$.

Theorem 11. *Let $\Phi(z) = \sum_{n\ge0} z^{3^n}$, and let α be a non-negative integer. Then the generating function $N(z)$, when reduced modulo 3^{3^α}, can be expressed as a polynomial in $\Phi(z)$ of degree at most $3^{\alpha+1}-1$, with coefficients that are Laurent polynomials in z over the integers.*

Remark. Computer experiments seem to indicate that the generating function $N(z)$ in Theorem 11, when reduced modulo 3^{3^α}, can in fact be expressed as a polynomial in $\Phi(z)$ of degree at most $3^{\alpha+1}-1$, with coefficients that are *polynomials* in z over the integers.

Proof of Theorem 11. We apply the method from Section 4. We start by substituting the Ansatz (4.3) in (5.2) and reducing the result modulo 3. In this way, we obtain

$$\sum_{i=0}^{3^{\alpha+1}-1} a_{i,1}^3(z)\Phi^{3i}(z) + \sum_{i=0}^{3^{\alpha+1}-1} a_{i,1}^2(z)\Phi^{2i}(z) \\ - \sum_{0\le i<j\le 3^{\alpha+1}-1} a_{i,1}(z)a_{j,1}(z)\Phi^{i+j}(z) + 2z^2 = 0 \quad \text{modulo } 3. \tag{5.3}$$

We claim that the following choices solve the above congruence:

$$a_{0,1}(z) = s_\alpha^2(z) + s_\alpha(z) \quad \text{modulo } 3,$$

$$a_{3^\alpha,1}(z) = 1 - s_\alpha(z) \quad \text{modulo } 3,$$
$$a_{2\cdot3^\alpha,1}(z) = 1 \quad \text{modulo } 3, \tag{5.4}$$

where $s_\alpha(z)=\sum_{k=0}^{\alpha-1}z^{3^k}$, with all other $a_{i,1}(z)$ vanishing. In order to verify the claim, we substitute our choices in (5.3). For the left-hand side, we obtain

$$\begin{aligned}\Phi^{2\cdot3^{\alpha+1}}(z)+\big(1-s_\alpha^3(z)\big)\,\Phi^{3^{\alpha+1}}(z)+s_\alpha^6(z)+s_\alpha^3(z)\\ +\Phi^{4\cdot3^\alpha}(z)+\big(1+s_\alpha^2(z)+s_\alpha(z)\big)\,\Phi^{2\cdot3^\alpha}(z)+s_\alpha^4(z)-s_\alpha^3(z)+s_\alpha^2(z)\\ -\left(1-s_\alpha(z)\right)\Phi^{3\cdot3^\alpha}(z)-\big(s_\alpha^2(z)+s_\alpha(z)\big)\,\Phi^{2\cdot3^\alpha}(z)-\big(s_\alpha(z)-s_\alpha^3(z)\big)\,\Phi^{3^\alpha}(z)+2z^2\\ \text{modulo }3.\end{aligned}$$

Using the relation (4.5) with $p=3$ and reducing the obtained expression modulo 3, we arrive at

$$\begin{aligned}\Phi^{2\cdot3^\alpha}(z)-2z^{3^\alpha}\Phi^{3^\alpha}(z)+z^{2\cdot3^\alpha}+\big(s_\alpha(z)-s_\alpha^3(z)\big)\left(\Phi^{3^\alpha}(z)-z^{3^\alpha}\right)\\ +\Phi^{3^\alpha}(z)\left(\Phi^{3^\alpha}(z)-z^{3^\alpha}\right)+\Phi^{2\cdot3^\alpha}(z)+s_\alpha^6(z)+s_\alpha^4(z)+s_\alpha^2(z)\\ -\big(s_\alpha(z)-s_\alpha^3(z)\big)\,\Phi^{3^\alpha}(z)+2z^2\\ =z^{2\cdot3^\alpha}-z^{3^\alpha}s_\alpha(z)+z^{3^\alpha}s_\alpha^3(z)+s_\alpha^6(z)+s_\alpha^4(z)+s_\alpha^2(z)-z^2\qquad\text{modulo }3.\end{aligned}$$

By using the relation

$$s_\alpha^3(z)=s_\alpha(z)+z^{3^\alpha}-z\qquad\text{modulo }3\tag{5.5}$$

several times, this expression can be turned into

$$\begin{aligned}z^{2\cdot3^\alpha}-z^{3^\alpha}s_\alpha(z)+z^{3^\alpha}\left(s_\alpha(z)+z^{3^\alpha}-z\right)+\left(s_\alpha(z)+z^{3^\alpha}-z\right)^2\\ +s_\alpha(z)\left(s_\alpha(z)+z^{3^\alpha}-z\right)+s_\alpha^2(z)-z^2\qquad\text{modulo }3.\end{aligned}$$

After expansion and reduction modulo 3, one sees that this expression reduces to zero.

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. We consider the Ansatz (4.6)–(4.8), where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution $F_\beta(z)=\sum_{i=0}^{3^{\alpha+1}-1}a_{i,\beta}(z)\Phi^i(z)$ to (5.2) modulo 3^β. This Ansatz, substituted in (5.2), produces the congruence

$$-3^\beta\sum_{j=0}^{3^{\alpha+1}-1}\sum_{i=0}^{3^{\alpha+1}-1}a_{j,\beta}(z)b_{i,\beta+1}(z)\Phi^{i+j}(z)+F_\beta^3(z)+F_\beta^2(z)-3zF_\beta(z)+2z^2=0\\ \text{modulo }3^{\beta+1}.\tag{5.6}$$

Since the sum has the prefactor 3^β, we may reduce the $a_{i,\beta}(z)$ modulo 3. By construction, we have

$$\begin{aligned}a_{0,\beta}(z)=a_{0,1}(z)=s^2(\alpha)+s_\alpha(z)\qquad\text{modulo }3,\\ a_{3^\alpha,\beta}(z)=a_{3^\alpha,1}(z)=1-s_\alpha(z)\qquad\text{modulo }3,\\ a_{2\cdot3^\alpha,\beta}(z)=a_{2\cdot3^\alpha,1}(z)=1\qquad\text{modulo }3,\end{aligned}$$

and $a_{i,\beta}=0$ modulo 3 for all other i's. If we substitute this in (5.6) and subsequently use (4.5) with $p=3$ to reduce high powers of $\Phi(z)$, we obtain

$$
\begin{aligned}
&-3^\beta\left(s_\alpha^2(z)+s_\alpha(z)\right)\sum_{i=0}^{3^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^i(z)-3^\beta\left(1-s_\alpha(z)\right)\sum_{i=0}^{3^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^{3^\alpha+i}(z)\\
&\qquad\qquad-3^\beta\sum_{i=0}^{3^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^{2\cdot 3^\alpha+i}(z)+F_\beta^3(z)+F_\beta^2(z)-3zF_\beta(z)+2z^2\\
&=-3^\beta\sum_{i=0}^{3^\alpha-1}\Big(\left(s_\alpha^2(z)+s_\alpha(z)\right)b_{i,\beta+1}(z)\\
&\qquad\qquad\qquad-\left(1-s_\alpha(z)\right)z^{3^\alpha}b_{i+2\cdot 3^\alpha,\beta+1}(z)-z^{3^\alpha}b_{i+3^\alpha,\beta+1}(z)\Big)\,\Phi^i(z)\\
&\quad-3^\beta\sum_{i=3^\alpha}^{2\cdot 3^\alpha-1}\Big(\left(s_\alpha^2(z)+s_\alpha(z)\right)b_{i,\beta+1}(z)+\left(1-s_\alpha(z)\right)b_{i-3^\alpha,\beta+1}(z)\\
&\qquad\qquad\qquad+\left(1-s_\alpha(z)\right)b_{i+3^\alpha,\beta+1}(z)+b_{i,\beta+1}(z)-z^{3^\alpha}b_{i+3^\alpha,\beta+1}(z)\Big)\,\Phi^i(z)\\
&\quad-3^\beta\sum_{i=2\cdot 3^\alpha}^{3^{\alpha+1}-1}\Big(\left(s_\alpha^2(z)+s_\alpha(z)\right)b_{i,\beta+1}(z)+\left(1-s_\alpha(z)\right)b_{i-3^\alpha,\beta+1}(z)\\
&\qquad\qquad\qquad\qquad+b_{i-2\cdot 3^\alpha,\beta+1}(z)+b_{i,\beta+1}(z)\Big)\,\Phi^i(z)\\
&\qquad\qquad\qquad+F_\beta^3(z)+F_\beta^2(z)-3zF_\beta(z)+2z^2=0\qquad\text{modulo } 3^{\beta+1}.
\end{aligned}
$$

By our assumption on $F_\beta(z)$, we may divide by 3^β. Comparison of powers of $\Phi(z)$ then yields a system of congruences of the form

$$M\cdot b=c\quad\text{modulo } 3,\tag{5.7}$$

where b is the column vector of unknowns $(b_{i,\beta+1}(z))_{i=0,1,\dots,3^{\alpha+1}-1}$, c is a (known) column vector of Laurent polynomials in z, and M is the matrix

$$
\begin{pmatrix}
D(s_\alpha^2(z)+s_\alpha(z)) & D(-z^{3^\alpha}) & D(-z^{3^\alpha}(1-s_\alpha(z)))\\
D(1-s_\alpha(z)) & D(s_\alpha^2(z)+s_\alpha(z)+1) & D(1-s_\alpha(z)-z^{3^\alpha})\\
D(1) & D(1-s_\alpha(z)) & D(s_\alpha^2(z)+s_\alpha(z)+1)
\end{pmatrix},
$$

with $D(x)$ denoting the $3^\alpha\times 3^\alpha$ diagonal matrix whose diagonal entries equal x. We claim that

$$\det(M)=z^{2\cdot 3^\alpha}\qquad\text{modulo } 3.$$

In order to see this, we subtract $s_\alpha^2(z)+s_\alpha(z)$ times row $i+2\cdot 3^\alpha$ from row i, $i=0,1,\dots,3^\alpha-1$, and we subtract $1-s_\alpha(z)$ times row $i+2\cdot 3^\alpha$ from row $i+3^\alpha$, $i=0,1,\dots,3^\alpha-1$. If, in addition, we move rows $2\cdot 3^\alpha,2\cdot 3^\alpha+1,\dots,3^{\alpha+1}-1$ to the top of the matrix, then it attains an upper triangular form, from which one infers that

$$
\begin{aligned}
\det(M)&=(-1)^{2\cdot 3^\alpha\cdot 3^\alpha}\det{}^2\big(D(s_\alpha^3(z)-s_\alpha(z)-z^{3^\alpha})\big)\det\big(D(1)\big)\\
&=\left(s_\alpha^3(z)-s_\alpha(z)-z^{3^\alpha}\right)^{2\cdot 3^\alpha}\\
&=z^{2\cdot 3^\alpha}\qquad\text{modulo } 3,
\end{aligned}
$$

by means of (5.5), as we claimed. As a consequence, the system (5.7) is (uniquely) solvable. Thus, we have proved that, for an arbitrary non-negative integer α, the algorithm of Section 4 will produce a solution $F_{3^\alpha}(z)$ to (5.2) modulo 3^{3^α} which is a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z. $\square$

We have implemented this algorithm. As an illustration, the next theorem contains the result for the modulus 27.

Theorem 12. *Let $\Phi(z) = \sum_{n\ge0} z^{3^n}$. Then we have*

$$\sum_{n\ge1} N_n\, z^n = 18z^3 + z^2 + z + (18z^3 + 12z^2)\Phi(z) + (3z^2 + 15z)\Phi^2(z) \\ + (9z^2 + 5z + 13)\Phi^3(z) + (9z^2 + 6z + 24)\Phi^4(z) + (15z + 6)\Phi^5(z) \\ + (18z + 4)\Phi^6(z) + (18z + 21)\Phi^7(z) + 12\Phi^8(z) \qquad \text{modulo } 27. \quad (5.8)$$

In [5, Conj. 5.18], Deutsch and Sagan conjectured that

$$N_n \equiv \begin{cases} 1 \pmod 3 & \text{if } n = 3^i \text{ or } n = 2\cdot 3^i \text{ for an integer } i \ge 0, \\ 2 \pmod 3 & \text{if } n = 3^{i_1} + 3^{i_2} \text{ for integers } i_1 > i_2 \ge 0, \\ 0 \pmod 3 & \text{otherwise.} \end{cases} \quad (5.9)$$

This conjecture was proved by Eu, Liu and Yeh [7] by carefully analysing a binomial sum formula for N_n modulo 3. A simpler proof was given by Gessel in [9]. It should be noted that his proof is essentially the one resulting from the $\alpha = 0$ case of Theorem 11. Moreover, our results allow us to generalise this — in principle — to any power of 3. For the sake of illustration, we display the results for the moduli $9 = 3^2$ and $27 = 3^3$.

Corollary 13. *The numbers N_n of connected non-crossing graphs obey the following congruences modulo* 27:

(i) $N_n \equiv 1 \pmod{27}$ *if, and only if,* $n = 1$, *or* $n = 2\cdot 3^i$ *with* $i \ge 0$;
(ii) $N_n \equiv 2 \pmod{27}$ *if, and only if,* $n = 10\cdot 3^i$ *with* $i \ge 1$;
(iii) $N_n \equiv 3 \pmod{27}$ *if, and only if,* $n = 2\cdot 3^i + 1$ *with* $i \ge 1$, *or* $n = 3^i + 2$ *with* $i \ge 1$, *or* $n = 2\cdot 3^{i_1} + 2\cdot 3^{i_2}$ *with* $i_1 > i_2 \ge 0$, *or* $n = 4\cdot 3^{i_1} + 3^{i_2} + 3^{i_3}$ *with* $i_1 - 2 > i_2 - 1 > i_3 \ge 0$, *or* $n = 3^{i_1} + 4\cdot 3^{i_2} + 3^{i_3}$ *with* $i_1 - 3 > i_2 - 1 > i_3 \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 4\cdot 3^{i_3}$ *with* $i_1 - 3 > i_2 - 2 > i_3 \ge 0$;
(iv) $N_n \equiv 4 \pmod{27}$ *if, and only if,* $n = 3$;
(v) $N_n \equiv 5 \pmod{27}$ *if, and only if,* $n = 4\cdot 3^i$ *with* $i \ge 1$;
(vi) $N_n \equiv 6 \pmod{27}$ *if, and only if,* $n = 22\cdot 3^i$ *with* $i \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 1$ *with* $i_1 - 1 > i_2 \ge 2$, *or* $n = 4\cdot 3^{i_1} + 3^{i_2}$ *with* $i_1 - 1 > i_2 \ge 1$, *or* $n = 3^{i_1} + 4\cdot 3^{i_2}$ *with* $i_1 - 2 > i_2 \ge 1$, *or* $n = 2\cdot 3^{i_1} + 3^{i_2} + 3^{i_3}$ *with* $i_1 - 2 > i_2 - 1 > i_3 \ge 0$, *or* $n = 3^{i_1} + 2\cdot 3^{i_2} + 3^{i_3}$ *with* $i_1 - 1 > i_2 - 1 > i_3 \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 2\cdot 3^{i_3}$ *with* $i_1 - 1 > i_2 > i_3 \ge 0$;
(vii) $N_n \equiv 9 \pmod{27}$ *if, and only if,* $n = 2\cdot 3^{i_1} + 2\cdot 3^{i_2} + 3^{i_3}$ *with* $i_1 > i_2 > i_3 \ge 0$, *or* $n = 2\cdot 3^{i_1} + 3^{i_2} + 2\cdot 3^{i_3}$ *with* $i_1 > i_2 > i_3 \ge 0$, *or* $n = 3^{i_1} + 2\cdot 3^{i_2} + 2\cdot 3^{i_3}$ *with* $i_1 > i_2 > i_3 \ge 0$, *or* $n = 2\cdot 3^{i_1} + 2\cdot 3^{i_2} + 2\cdot 3^{i_3}$ *with* $i_1 > i_2 > i_3 \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4} + 3^{i_5}$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 0$,
or $n = 2\cdot 3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4} + 3^{i_5}$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 0$, *or* $n = 3^{i_1} + 2\cdot 3^{i_2} + 3^{i_3} + 3^{i_4} + 3^{i_5}$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 2\cdot 3^{i_3} + 3^{i_4} + 3^{i_5}$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 3^{i_3} + 2\cdot 3^{i_4} + 3^{i_5}$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4} + 2\cdot 3^{i_5}$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 0$;

(viii) $N_n \equiv 11 \pmod{27}$ *if, and only if,* $n = 3^i + 1$ *with* $i \geq 3$;

(ix) $N_n \equiv 12 \pmod{27}$ *if, and only if,* $n = 7$; *or* $n = 40 \cdot 3^i$ *with* $i \geq 0$, *or* $n = 2 \cdot 3^{i_1} + 3^{i_2} + 1$ *with* $i_1 - 1 > i_2 \geq 1$, *or* $n = 3^{i_1} + 2 \cdot 3^{i_2} + 1$ *with* $i_1 - 1 > i_2 \geq 1$, *or* $n = 3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4}$ *with* $i_1 - 3 > i_2 - 2 > i_3 - 1 > i_4 \geq 0$;

(x) $N_n \equiv 13 \pmod{27}$ *if, and only if,* $n = 3^i$ *with* $i \geq 2$;

(xi) $N_n \equiv 15 \pmod{27}$ *if, and only if,* $n = 3^i + 4$ *with* $i \geq 3$, *or* $n = 4 \cdot 3^i + 1$ *with* $i \geq 2$, *or* $n = 13 \cdot 3^i$ *with* $i \geq 1$, *or* $n = 4 \cdot 3^{i_1} + 2 \cdot 3^{i_2}$ *with* $i_1 - 1 > i_2 \geq 0$, *or* $n = 2 \cdot 3^{i_1} + 4 \cdot 3^{i_2}$ *with* $i_1 - 2 > i_2 \geq 0$;

(xii) $N_n \equiv 18 \pmod{27}$ *if, and only if,* $n = 2 \cdot 3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 3^{i_1} + 2 \cdot 3^{i_2} + 3^{i_3} + 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 3^{i_1} + 3^{i_2} + 2 \cdot 3^{i_3} + 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 3^{i_1} + 3^{i_2} + 3^{i_3} + 2 \cdot 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 2 \cdot 3^{i_1} + 2 \cdot 3^{i_2} + 3^{i_3} + 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 2 \cdot 3^{i_1} + 3^{i_2} + 2 \cdot 3^{i_3} + 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 2 \cdot 3^{i_1} + 3^{i_2} + 3^{i_3} + 2 \cdot 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 3^{i_1} + 2 \cdot 3^{i_2} + 2 \cdot 3^{i_3} + 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 3^{i_1} + 2 \cdot 3^{i_2} + 3^{i_3} + 2 \cdot 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 3^{i_1} + 3^{i_2} + 2 \cdot 3^{i_3} + 2 \cdot 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \geq 0$, *or* $n = 3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4} + 3^{i_5} + 3^{i_6}$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 > i_6 \geq 0$;

(xiii) $N_n \equiv 20 \pmod{27}$ *if, and only if,* $n = 10$, *or* $n = 3^{i_1} + 3^{i_2}$ *with* $i_1 - 2 > i_2 \geq 1$;

(xiv) $N_n \equiv 21 \pmod{27}$ *if, and only if,* $n = 7 \cdot 3^i$ *with* $i \geq 1$, *or* $n = 4 \cdot 3^{i_1} + 4 \cdot 3^{i_2}$ *with* $i_1 - 2 > i_2 \geq 0$, *or* $n = 13 \cdot 3^{i_1} + 3^{i_2}$ *with* $i_1 - 1 > i_2 \geq 0$, *or* $n = 3^{i_1} + 13 \cdot 3^{i_2}$ *with* $i_1 - 3 > i_2 \geq 0$;

(xv) $N_n \equiv 23 \pmod{27}$ *if, and only if,* $n = 4$;

(xvi) $N_n \equiv 24 \pmod{27}$ *if, and only if,* $n = 13$, *or* $n = 16 \cdot 3^i$ *with* $i \geq 0$, *or* $n = 7 \cdot 3^{i_1} + 3^{i_2}$ *with* $i_1 - 1 > i_2 \geq 0$;

(xvii) *in the cases not covered by items* (i)–(xvi), N_n *is divisible by* 27; *in particular,* $N_n \not\equiv 7, 8, 10, 14, 16, 17, 19, 22, 25, 26 \pmod{27}$ *for all* n.

Proof. We convert the right-hand side of (5.8) into a linear combination of series $H_{a_1,a_2,\dots,a_r}(z)$ with all a_i's relatively prime to p, by means of Equation (3.1) and Proposition 9. The result is

$$\begin{aligned}\sum_{n\geq 1} N_n\, z^n = 9z^2 + 15z + (18z+13)H_1(z) + (18z+1)H_2(z) + (9z+20)H_{1,1}(z)\\
+ 12H_{2,1}(z) + 12H_{1,2}(z) + 24H_{1,1,1}(z) + 12H_4(z) + 3H_{2,2}(z)\\
+ 6H_{2,1,1}(z) + 6H_{1,2,1}(z) + 6H_{1,1,2}(z) + 12H_{1,1,1,1}(z) + 9H_{4,1}(z) + 9H_{1,4}(z)\\
+ 9H_{2,2,1}(z) + 9H_{2,1,2}(z) + 9H_{1,2,2}(z) + 18H_{2,1,1,1}(z) + 18H_{1,2,1,1}(z)\\
+ 18H_{1,1,2,1}(z) + 18H_{1,1,1,2}(z) + 9H_{1,1,1,1,1}(z) + 9H_{4,2}(z) + 9H_{2,4}(z)\\
+ 18H_{4,1,1}(z) + 18H_{1,4,1}(z) + 18H_{1,1,4}(z) + 9H_{2,2,2}(z) + 18H_{2,2,1,1}(z) + 18H_{2,1,2,1}(z)\\
+ 18H_{2,1,1,2}(z) + 18H_{1,2,2,1}(z) + 18H_{1,2,1,2}(z) + 18H_{1,1,2,2}(z)\\
+ 9H_{2,1,1,1,1}(z) + 9H_{1,2,1,1,1}(z) + 9H_{1,1,2,1,1}(z)\\
+ 9H_{1,1,1,2,1}(z) + 9H_{1,1,1,1,2}(z) + 18H_{1,1,1,1,1,1}(z) \qquad \text{modulo } 27.\end{aligned}$$

Coefficient extraction following the algorithm described in Remark 8 then yields the claimed congruences. ☐

Considered modulo 9, the above corollary reduces to the following.

Corollary 14. *The numbers N_n of connected non-crossing graphs obey the following congruences modulo* 9:

(i) $N_n \equiv 1 \pmod 9$ *if, and only if,* $n = 1$, *or* $n = 2 \cdot 3^i$ *with* $i \ge 0$;
(ii) $N_n \equiv 2 \pmod 9$ *if, and only if,* $n = 3^{i_1} + 3^{i_2}$ *with* $i_1 - 1 > i_2 \ge 0$;
(iii) $N_n \equiv 3 \pmod 9$ *if, and only if,* $n = 2\cdot 3^{i_1} + 3^{i_2}$ *with* $i_1 > i_2 \ge 0$, *or* $n = 3^{i_1} + 2\cdot 3^{i_2}$ *with* $i_1 > i_2 \ge 0$, *or* $n = 2\cdot 3^{i_1} + 2\cdot 3^{i_2}$ *with* $i_1 > i_2 \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4}$ *with* $i_1 > i_2 > i_3 > i_4 \ge 0$;
(iv) $N_n \equiv 4 \pmod 9$ *if, and only if,* $n = 3^i$ *with* $i \ge 0$;
(v) $N_n \equiv 5 \pmod 9$ *if, and only if,* $n = 4 \cdot 3^i$ *with* $i \ge 0$;
(vi) $N_n \equiv 6 \pmod 9$ *if, and only if,* $n = 3^{i_1} + 3^{i_2} + 3^{i_3}$ *with* $i_1 > i_2 > i_3 \ge 0$, *or* $n = 2 \cdot 3^{i_1} + 3^{i_2} + 3^{i_3}$ *with* $i_1 > i_2 > i_3 \ge 0$, *or* $n = 3^{i_1} + 2 \cdot 3^{i_2} + 3^{i_3}$ *with* $i_1 > i_2 > i_3 \ge 0$, *or* $n = 3^{i_1} + 3^{i_2} + 2 \cdot 3^{i_3}$ *with* $i_1 > i_2 > i_3 \ge 0$;
(vi) *in the cases not covered by items* (i)–(vii), N_n *is divisible by* 9; *in particular,* $N_n \not\equiv 7, 8 \pmod 9$ *for all* n.

Remark. In the first proof of the conjecture (5.9) in [7], Eu, Liu and Yeh worked from the sum expression

$$N_n = \frac{1}{n-1} \sum_{i=n-2}^{2n-4} \binom{3n-3}{n+i+1} \binom{i}{n-2}$$

which is provided in [8, Theorem 2]. In order to achieve the proof, they considered four auxiliary sums of very similar nature, called there $f_i(n)$, $i = 1, 2, 3, 4$, of which they determined their behaviour modulo 3. These sums, and the numbers N_n of connected non-crossing graphs, are reconsidered by Gessel in [9], who provides simpler proofs of the congruences modulo 3 established in [7], and also closed form expressions for the sums $f_i(n)$, $i = 1, 2, 3, 4$. Gessel adds another sum, called $f_5(n)$, of which he also determines its behaviour modulo 3.

All these sums can be treated in the same way as the numbers N_n in Theorems 11, 12, and Corollaries 13, 14, as we are going to explain now. In particular, in this way the behaviour of any of $f_i(n)$, $i = 1, 2, 3, 4, 5$, modulo *any* power of 3 can be determined.

The general family of sums introduced by Gessel in [9] is

$$g_{j,k,l}(n) = \sum_{i=n-l}^{2n+j-k} \binom{3n+j}{n+i+k} \binom{i}{n-l},$$

of which the sums $f_i(n)$, $i = 1, 2, 3, 4, 5$, are the cases $(j, k, l) = (1, 1, 0)$, $(0, 1, 0)$, $(0, 0, 0)$, $(-1, 1, 1)$, $(0, 1, 1)$, in this order. Gessel [9, Sec. 3] proves that the generating function

$$G_{j,k,l}(z) = \sum_{n=k-j-l}^{\infty} g_{j,k,l}(n) z^n$$

for these sums is given by

$$G_{j,k,l}(z) = \frac{(1 - 2\alpha(z))^l \, \alpha^{k-j-l}(z)}{(1 - 6\alpha(z) + 6\alpha^2(z))\,(1 - \alpha(z))^{k-1}},$$

where $\alpha(z)$ is the compositional inverse of $z(1 - z)(1 - 2z)$. The series $\alpha(z)$ thus being algebraic of degree 3, also all series $G_{j,k,l}(z)$ are algebraic of degree 3. Below we list the algebraic equations satisfied by the generating functions for $f_i(n)$, $i = 1, 2, 3, 4, 5$, and in each case we provide the base solution $F_1(z)$ for the modulus 3^{3^α} (cf. (4.3) with

$p = 3$) for starting our method described in Section 4. The iterative steps carry through as well, as in the proof of Theorem 11. We leave the details to the reader.

The generating function for the numbers $f_1(n)$ satisfies the equation

$$(1 - 108z^2)G_{1,1,0}^3(z) - 3G_{1,1,0}(z) + 2 = 0. \tag{5.10}$$

A base solution for the modulus 3^{3^α} is $F_1(z) = 1$. The generating function for the numbers $f_2(n)$ satisfies the equation

$$(1 - 108z^2)G_{0,1,0}^3(z) - (1 + 9z)G_{0,1,0}(z) + z = 0, \tag{5.11}$$

and a base solution is $F_1(z) = \Phi^{3^\alpha}(z) + s_\alpha(z)$. Next, the generating function for the numbers $f_3(n)$ satisfies the equation

$$(1 - 108z^2)G_{0,0,0}^3(z) - (1 + 9z)G_{0,0,0}(z) - z = 0. \tag{5.12}$$

Here, a base solution is $F_1(z) = -\Phi^{3^\alpha}(z) - s_\alpha(z) + 1$. The generating function for the numbers $f_4(n)$ satisfies the equation

$$(1-108z^2)G_{-1,1,1}^3(z) + (1-108z^2)G_{-1,1,1}^2(z) + 3z(1-12z)G_{-1,1,1}(z) - 4z^2 = 0. \tag{5.13}$$

Since, modulo 3, this is the same equation as (5.2), this generating function has the same base solution as $N(z)$, namely the one given by (5.4). Finally, the generating function for the numbers $f_5(n)$ satisfies the equation

$$(1 - 108z^2)G_{0,1,1}^3(z) - G_{0,1,1}(z) - 8z = 0. \tag{5.14}$$

Since, modulo 3, this is the same equation as (5.11), (essentially) the same base solution (the difference occurring in the constant term), namely $F_1(z) = \Phi^{3^\alpha}(z) + s_\alpha(z) + 1$, applies.

6. The number of Kreweras walks modulo 3-powers

The subject of this section are congruences modulo powers of 3 for the numbers of so-called "Kreweras walks." In his thesis [14], Kreweras had considered (among many other things) a three-candidate ballot problem, where each of the three candidates, A, B, C, say, receives n votes. The problem which is posed is how many ways there are to count the votes so that at each point in time candidate A has at least as many votes as the number of votes for each of the other candidates. It is not difficult to see that this problem can be translated into the following problem of counting walks in the quarter plane: how many lattice walks in the plane from the origin to itself are there which consist of $3n$ steps from the set $\{(1,1), (-1,0), (0,-1)\}$ and stay in the non-negative quadrant? Let K_n denote the number of these walks. By definition, we set $K_0 = 1$. Kreweras [14] proved that

$$K_n = \frac{4^n}{(n+1)(2n+1)}\binom{3n}{n}; \tag{6.1}$$

see also [16]. To prove this formula turned out to be highly non-trivial, as well as the enumerative analysis of the more general question of how many walks there are which end at an arbitrary point in the non-negative quadrant. Kreweras [14] and Niederhausen [16] obtained partial results in this direction. Finally, Bousquet-Mélou [2] succeeded to compute the complete generating function for these numbers of walks.

Let $K(z) := \sum_{n\ge0} K_n\, z^n$ be the generating function for the "Kreweras numbers" in (6.1). From [2, Theorem 1], it can be derived that

$$64z^2\, K^3(z) + 16z\, K^2(z) - (72z-1)\, K(z) + 54z - 1 = 0. \tag{6.2}$$

Clearly, this equation determines $K(z)$ uniquely as a formal power series over $\mathbb{Z}$, and as well modulo any power of 3.

Theorem 15. *Let $\Phi(z) = \sum_{n\ge0} z^{3^n}$, and let α be a non-negative integer. Then the generating function $K(z)$, when reduced modulo 3^{3^α}, can be expressed as a polynomial in $\Phi(z^{1/2})$ of degree at most $3^{\alpha+1}-1$, with coefficients that are Laurent polynomials in $z^{1/2}$ over the integers.*

Proof. We apply the method from Section 4. We start by substituting the Ansatz (4.3) with z replaced by $z^{1/2}$ in (6.2) and reducing the result modulo 3. In this way, we obtain

$$z^2 \sum_{i=0}^{3^{\alpha+1}-1} a_{i,1}^3(z^{1/2})\Phi^{3i}(z^{1/2}) + z \sum_{i=0}^{3^{\alpha+1}-1} a_{i,1}^2(z^{1/2})\Phi^{2i}(z^{1/2}) \\ - z \sum_{0\le i<j\le 3^{\alpha+1}-1} a_{i,1}(z^{1/2})a_{j,1}(z^{1/2})\Phi^{i+j}(z^{1/2}) \\ + \sum_{i=0}^{3^{\alpha+1}-1} a_{i,1}(z^{1/2})\Phi^{i}(z^{1/2}) - 1 = 0 \quad \text{modulo } 3. \tag{6.3}$$

We claim that the following choices solve the above congruence:

$$\begin{aligned} a_{0,1}(z^{1/2}) &= z^{-1}s_\alpha^2(z^{1/2}) \quad \text{modulo } 3,\\ a_{3^\alpha,1}(z^{1/2}) &= -z^{-1}s_\alpha(z^{1/2}) \quad \text{modulo } 3,\\ a_{2\cdot3^\alpha,1}(z^{1/2}) &= z^{-1} \quad \text{modulo } 3, \end{aligned}$$

where $s_\alpha(z)$ is the same polynomial as in Section 5, with all other $a_{i,1}(z^{1/2})$ vanishing. In order to verify the claim, we substitute our choices in (6.3). For the left-hand side, we obtain

$$z^2\left(z^{-3}\Phi^{2\cdot3^{\alpha+1}}(z^{1/2}) - z^{-3}s_\alpha^3(z^{1/2})\Phi^{3^{\alpha+1}}(z^{1/2}) + z^{-3}s_\alpha^6(z^{1/2})\right) \\ + z\left(z^{-2}\Phi^{4\cdot3^\alpha}(z^{1/2}) + z^{-2}s_\alpha^2(z^{1/2})\Phi^{2\cdot3^\alpha}(z^{1/2}) + z^{-2}s_\alpha^4(z^{1/2})\right) \\ - z\left(-z^{-2}s_\alpha(z^{1/2})\Phi^{3^{\alpha+1}}(z^{1/2}) + z^{-2}s_\alpha^2(z^{1/2})\Phi^{2\cdot3^\alpha}(z^{1/2}) - z^{-2}s_\alpha^3(z^{1/2})\Phi^{3^\alpha}(z^{1/2})\right) \\ + z^{-1}\Phi^{2\cdot3^\alpha}(z^{1/2}) - z^{-1}s_\alpha(z^{1/2})\Phi^{3^\alpha}(z^{1/2}) + z^{-1}s_\alpha^2(z^{1/2}) - 1 \qquad \text{modulo } 3.$$

Using the relation (4.5) with $p=3$ and z replaced by $z^{1/2}$, and reducing the obtained expression modulo 3, we arrive at

$$\begin{aligned}\Big(z^{-1}\Phi^{2\cdot 3^\alpha}(z^{1/2})+\Phi^{3^\alpha}(z^{1/2})z^{3^\alpha/2-1}+z^{3^\alpha-1}\Big)&\\
-\Big(z^{-1}s_\alpha^3(z^{1/2})\Phi^{3^\alpha}(z^{1/2})-z^{3^\alpha/2-1}s_\alpha^3(z^{1/2})\Big)+z^{-1}s_\alpha^6(z^{1/2})&\\
+\Big(z^{-1}\Phi^{2\cdot 3^\alpha}(z^{1/2})-z^{3^\alpha/2-1}\Phi^{3^\alpha}(z^{1/2})\Big)+z^{-1}s_\alpha^2(z^{1/2})\Phi^{2\cdot 3^\alpha}(z^{1/2})+z^{-1}s_\alpha^4(z^{1/2})&\\
+\Big(z^{-1}s_\alpha(z^{1/2})\Phi^{3^\alpha}(z^{1/2})-z^{3^\alpha/2-1}s_\alpha(z^{1/2})\Big)&\\
-z^{-1}s_\alpha^2(z^{1/2})\Phi^{2\cdot 3^\alpha}(z^{1/2})+z^{-1}s_\alpha^3(z^{1/2})\Phi^{3^\alpha}(z^{1/2})&\\
+z^{-1}\Phi^{2\cdot 3^\alpha}(z^{1/2})-z^{-1}s_\alpha(z^{1/2})\Phi^{3^\alpha}(z^{1/2})+z^{-1}s_\alpha^2(z^{1/2})-1&\quad\text{modulo } 3.\end{aligned}$$

By collecting terms, this expression simplifies to

$$\begin{aligned}z^{3^\alpha-1}+z^{3^\alpha/2-1}s_\alpha^3(z^{1/2})+z^{-1}s_\alpha^6(z^{1/2})+z^{-1}s_\alpha^4(z^{1/2})&\\
-z^{3^\alpha/2-1}s_\alpha(z^{1/2})+z^{-1}s_\alpha^2(z^{1/2})-1&\quad\text{modulo } 3.\end{aligned}$$

By repeatedly using the relation (5.5) with z replaced by $z^{1/2}$, this expression can be turned into

$$\begin{aligned}&z^{3^\alpha-1}+z^{3^\alpha/2-1}\left(s_\alpha(z^{1/2})+z^{3^\alpha/2}-z^{1/2}\right)+z^{-1}\left(s_\alpha(z^{1/2})+z^{3^\alpha/2}-z^{1/2}\right)^2\\
&+z^{-1}s_\alpha(z^{1/2})\left(s_\alpha(z^{1/2})+z^{3^\alpha/2}-z^{1/2}\right)-z^{3^\alpha/2-1}s_\alpha(z^{1/2})+z^{-1}s_\alpha^2(z^{1/2})-1\quad\text{modulo } 3.\end{aligned}$$

After expansion and reduction modulo 3, one sees that this expression reduces to zero.

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. We consider the Ansatz (4.6)–(4.8) with z replaced by $z^{1/2}$, where the coefficients $a_{i,\beta}(z^{1/2})$ are supposed to provide a solution

$$F_\beta(z)=\sum_{i=0}^{3^{\alpha+1}-1}a_{i,\beta}(z^{1/2})\Phi^i(z^{1/2})$$

to (5.2) modulo 3^β. This Ansatz, substituted in (5.2), produces the congruence

$$\begin{aligned}-3^\beta z\sum_{j=0}^{3^{\alpha+1}-1}\sum_{i=0}^{3^{\alpha+1}-1}a_{j,\beta}(z^{1/2})b_{i,\beta+1}(z^{1/2})\Phi^{i+j}(z^{1/2})+3^\beta\sum_{i=0}^{3^{\alpha+1}-1}b_{i,\beta+1}(z^{1/2})\Phi^i(z^{1/2})&\\
+64z^2F_\beta^3(z)+16zF_\beta^2(z)-(72z-1)F_\beta(z)+54z-1=0\quad\text{modulo } 3^{\beta+1}.&\qquad(6.4)\end{aligned}$$

Since the sum has the prefactor 3^β, we may reduce the $a_{i,\beta}(z^{1/2})$ modulo 3. By construction, we have

$$\begin{aligned}a_{0,\beta}(z^{1/2})=a_{0,1}(z^{1/2})&=z^{-1}s_\alpha^2(z^{1/2})\quad\text{modulo } 3,\\
a_{3^\alpha,\beta}(z^{1/2})=a_{3^\alpha,1}(z^{1/2})&=-z^{-1}s_\alpha(z^{1/2})\quad\text{modulo } 3,\\
a_{2\cdot 3^\alpha,\beta}(z^{1/2})=a_{2\cdot 3^\alpha,1}(z^{1/2})&=z^{-1}\quad\text{modulo } 3,\end{aligned}$$

and $a_{i,\beta} = 0$ modulo 3 for all other i's. If we substitute this in (6.4) and subsequently use (4.5) with $p = 3$ and z replaced by $z^{1/2}$ to reduce high powers of $\Phi(z^{1/2})$, we obtain

$$
\begin{aligned}
&- 3^\beta \sum_{i=0}^{3^{\alpha+1}-1} s_\alpha^2(z^{1/2}) b_{i,\beta+1}(z^{1/2}) \Phi^i(z^{1/2}) + 3^\beta \sum_{i=0}^{3^{\alpha+1}-1} s_\alpha(z^{1/2}) b_{i,\beta+1}(z^{1/2}) \Phi^{i+3^\alpha}(z^{1/2}) \\
&\qquad - 3^\beta \sum_{i=0}^{3^{\alpha+1}-1} b_{i,\beta+1}(z^{1/2}) \Phi^{i+2\cdot 3^\alpha}(z^{1/2}) + 3^\beta \sum_{i=0}^{3^{\alpha+1}-1} b_{i,\beta+1}(z^{1/2}) \Phi^i(z^{1/2}) \\
&\qquad\qquad + 64z^2 F_\beta^3(z) + 16z F_\beta^2(z) - (72z-1) F_\beta(z) + 54z - 1 \\
&= -3^\beta \sum_{i=0}^{3^\alpha-1} \big(s_\alpha^2(z^{1/2}) b_{i,\beta+1}(z^{1/2}) + z^{3^\alpha/2} s_\alpha(z^{1/2}) b_{i+2\cdot 3^\alpha,\beta+1}(z^{1/2}) \\
&\qquad\qquad - z^{3^\alpha/2} b_{i+3^\alpha,\beta+1}(z^{1/2}) - b_{i,\beta+1}(z^{1/2}) \big) \Phi^i(z^{1/2}) \\
&\quad - 3^\beta \sum_{i=3^\alpha}^{2\cdot 3^\alpha-1} \big(s_\alpha^2(z^{1/2}) b_{i,\beta+1}(z^{1/2}) - s_\alpha(z^{1/2}) b_{i-3^\alpha,\beta+1}(z^{1/2}) \\
&\qquad\qquad - s_\alpha(z^{1/2}) b_{i+3^\alpha,\beta+1}(z^{1/2}) - z^{3^\alpha/2} b_{i+3^\alpha,\beta+1}(z^{1/2}) \big) \Phi^i(z^{1/2}) \\
&- 3^\beta \sum_{i=2\cdot 3^\alpha}^{3^{\alpha+1}-1} \big(s_\alpha^2(z^{1/2}) b_{i,\beta+1}(z^{1/2}) - s_\alpha(z^{1/2}) b_{i-3^\alpha,\beta+1}(z^{1/2}) + b_{i-2\cdot 3^\alpha,\beta+1}(z^{1/2}) \big) \Phi^i(z^{1/2}) \\
&\qquad + 64z^2 F_\beta^3(z) + 16z F_\beta^2(z) - (72z-1) F_\beta(z) + 54z - 1 = 0 \qquad \text{modulo } 3^{\beta+1}.
\end{aligned}
$$

By our assumption on $F_\beta(z)$, we may divide by 3^β. Comparison of powers of $\Phi(z^{1/2})$ then yields a system of congruences of the form

$$M \cdot b = c \quad \text{modulo } 3, \tag{6.5}$$

where b is the column vector of unknowns $(b_{i,\beta+1}(z^{1/2}))_{i=0,1,\dots,3^{\alpha+1}-1}$, c is a (known) column vector of Laurent polynomials in z, and M is the matrix

$$
\begin{pmatrix}
D\left(s_\alpha^2(z^{1/2}) - 1\right) & D\left(-z^{3^\alpha/2}\right) & D\left(z^{3^\alpha/2} s_\alpha(z^{1/2})\right) \\
D\left(-s_\alpha(z^{1/2})\right) & D\left(s_\alpha^2(z^{1/2})\right) & D\left(-s_\alpha(z^{1/2}) - z^{3^\alpha/2}\right) \\
D(1) & D\left(-s_\alpha(z^{1/2})\right) & D\left(s_\alpha^2(z^{1/2})\right)
\end{pmatrix},
$$

with $D(x)$ denoting the $3^\alpha \times 3^\alpha$ diagonal matrix whose diagonal entries equal x, as before. In the same manner as in the proof of Theorem 11, on sees that

$$\det(M) = z^{3^\alpha} \qquad \text{modulo } 3.$$

As a consequence, the system (6.5) is (uniquely) solvable. Thus, we have proved that, for an arbitrary non-negative integer α, the algorithm of Section 4 will produce a solution $F_{3^\alpha}(z)$ to (5.2) modulo 3^{3^α} which is a polynomial in $\Phi(z^{1/2})$ with coefficients that are Laurent polynomials in z. □

We have implemented this algorithm. As an illustration, the next theorem contains the result for the modulus 27.

Theorem 16. *Let* $\Phi(z) = \sum_{n\ge0} z^{3^n}$. *Then we have*

$$\sum_{n\ge0} K_n\,z^n = 1 + 12\Phi^2(z^{1/2}) + 11z^{-1/2}\Phi^3(z^{1/2}) + 6z^{-1}\Phi^4(z^{1/2}) + 15z^{-1/2}\Phi^5(z^{1/2}) \\ + z^{-1}\Phi^6(z^{1/2}) + 3z^{-1}\Phi^8(z^{1/2}) \qquad \text{modulo } 27. \quad (6.6)$$

Corollary 17. *The numbers K_n of Kreweras walks obey the following congruences modulo* 27:

(i) $K_n \equiv 1 \pmod{27}$ *if, and only if,* $n = 0$;
(ii) $K_n \equiv 2 \pmod{27}$ *if, and only if,* $n = 1$;
(iii) $K_n \equiv 3 \pmod{27}$ *if, and only if,* $n = 3^i$ *with* $i \ge 1$, *or* $n = \frac{1}{2}(13 \cdot 3^i - 1)$ *with* $i \ge 2$, *or* $n = \frac{1}{2}(3^i + 11)$ *with* $i \ge 4$, *or* $n = 2 \cdot 3^i + 1$ *with* $i \ge 3$, *or* $n = 20 \cdot 3^i - 1$ *with* $i \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4} - 2)$ *with* $i_1 - 3 > i_2 - 2 > i_3 - 1 > i_4 \ge 1$;
(iv) $K_n \equiv 5 \pmod{27}$ *if, and only if,* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} - 2)$ *with* $i_1 - 2 > i_2 \ge 2$;
(v) $K_n \equiv 6 \pmod{27}$ *if, and only if,* $n = 3^i + 1$ *with* $i \ge 3$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2})$ *with* $i_1 - 2 > i_2 \ge 1$, *or* $n = \frac{1}{2}(7 \cdot 3^{i_1} + 3^{i_2} - 2)$ *with* $i_1 - 1 > i_2 \ge 1$; *or* $n = \frac{1}{2}(3^{i_1} + 7 \cdot 3^{i_2} - 2)$ *with* $i_1 - 1 > i_2 \ge 1$;
(vi) $K_n \equiv 7 \pmod{27}$ *if, and only if,* $n = 3^i - 1$ *with* $i \ge 2$;
(vii) $K_n \equiv 8 \pmod{27}$ *if, and only if,* $n = 4$, *or* $n = 2 \cdot 3^i - 1$ *with* $i \ge 2$;
(viii) $K_n \equiv 9 \pmod{27}$ *if, and only if,* $n = 3^{i_1} + 3^{i_2} + 3^{i_3} - 1$ *with* $i_1 > i_2 > i_3 \ge 1$, *or* $n = \frac{1}{2}(2 \cdot 3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4} + 3^{i_5} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 2 \cdot 3^{i_2} + 3^{i_3} + 3^{i_4} + 3^{i_5} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 2 \cdot 3^{i_3} + 3^{i_4} + 3^{i_5} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 3^{i_3} + 2 \cdot 3^{i_4} + 3^{i_5} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4} + 2 \cdot 3^{i_5} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 \ge 1$;
(ix) $K_n \equiv 12 \pmod{27}$ *if, and only if,* $n = \frac{1}{2}(4 \cdot 3^{i_1} + 3^{i_2} - 1)$ *with* $i_1 - 1 > i_2 \ge 2$, *or* $n = \frac{1}{2}(3^{i_1} + 4 \cdot 3^{i_2} - 1)$ *with* $i_1 - 2 > i_2 \ge 2$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 2)$ *with* $i_1 - 2 > i_2 \ge 3$, *or* $n = \frac{1}{2}(13 \cdot 3^{i_1} + 3^{i_2} - 2)$ *with* $i_1 - 1 > i_2 \ge 1$, *or* $n = 2 \cdot 3^{i_1} + 2 \cdot 3^{i_2} - 1$ *with* $i_1 - 2 > i_2 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 13 \cdot 3^{i_2} - 2)$ *with* $i_1 - 3 > i_2 \ge 1$;
(x) $K_n \equiv 14 \pmod{27}$ *if, and only if,* $n = \frac{1}{2}(3^i + 1)$ *with* $i \ge 4$, *or* $n = 5 \cdot 3^i - 1$ *with* $i \ge 2$;
(xi) $K_n \equiv 15 \pmod{27}$ *if, and only if,* $n = \frac{1}{2}(7 \cdot 3^i - 1)$ *with* $i \ge 2$, *or* $n = \frac{1}{2}(3^i + 5)$ *with* $i \ge 2$, *or* $n = 2 \cdot 3^i$ *with* $i \ge 1$, *or* $n = 11 \cdot 3^i - 1$ *with* $i \ge 1$, *or* $n = \frac{1}{2}(2 \cdot 3^{i_1} + 3^{i_2} + 3^{i_3} - 2)$ *with* $i_1 - 2 > i_2 - 1 > i_3 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 2 \cdot 3^{i_2} + 3^{i_3} - 2)$ *with* $i_1 - 1 > i_2 - 1 > i_3 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 2 \cdot 3^{i_3} - 2)$ *with* $i_1 - 1 > i_2 > i_3 \ge 1$;
(xii) $K_n \equiv 16 \pmod{27}$ *if, and only if,* $n = 2$;
(xiii) $K_n \equiv 17 \pmod{27}$ *if, and only if,* $n = 5$;
(xiv) $K_n \equiv 18 \pmod{27}$ *if, and only if, or* $n = \frac{1}{2}(2 \cdot 3^{i_1} + 2 \cdot 3^{i_2} + 3^{i_3} + 3^{i_4} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 \ge 1$, *or* $n = \frac{1}{2}(2 \cdot 3^{i_1} + 3^{i_2} + 2 \cdot 3^{i_3} + 3^{i_4} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 \ge 1$, *or* $n = \frac{1}{2}(2 \cdot 3^{i_1} + 3^{i_2} + 3^{i_3} + 2 \cdot 3^{i_4} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 2 \cdot 3^{i_2} + 2 \cdot 3^{i_3} + 3^{i_4} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 2 \cdot 3^{i_2} + 3^{i_3} + 2 \cdot 3^{i_4} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 2 \cdot 3^{i_3} + 2 \cdot 3^{i_4} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 3^{i_3} + 3^{i_4} + 3^{i_5} + 3^{i_6} - 2)$ *with* $i_1 > i_2 > i_3 > i_4 > i_5 > i_6 \ge 1$;

(xv) $K_n \equiv 21 \pmod{27}$ *if, and only if,* $n = 19$, *or* $n = 3^{i_1}+3^{i_2}-1$ *with* $i_1 > i_2 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1}+3^{i_2}+3^{i_3}-1)$ *with* $i_1-2 > i_2-1 > i_3 \ge 2$, *or* $n = \frac{1}{2}(4\cdot 3^{i_1}+3^{i_2}+3^{i_3}-2)$ *with* $i_1 - 2 > i_2 - 1 > i_3 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 4 \cdot 3^{i_2} + 3^{i_3} - 2)$ *with* $i_1 - 3 > i_2 - 1 > i_3 \ge 1$, *or* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} + 4 \cdot 3^{i_3} - 2)$ *with* $i_1 - 3 > i_2 - 2 > i_3 \ge 1$;

(xvi) $K_n \equiv 23 \pmod{27}$ *if, and only if,* $n = 14$;

(xvii) $K_n \equiv 24 \pmod{27}$ *if, and only if,* $n = 10$, *or* $n = \frac{1}{2}(2 \cdot 3^{i_1} + 3^{i_2} - 1)$ *with* $i_1 - 1 > i_2 \ge 2$, *or* $n = \frac{1}{2}(3^{i_1} + 2\cdot 3^{i_2} - 1)$ *with* $i_1 > i_2 \ge 2$, *or* $n = 3^{i_1} + 2\cdot 3^{i_2} - 1$ *with* $i_1 - 2 > i_2 \ge 1$, *or* $n = 2 \cdot 3^{i_1} + 3^{i_2} - 1$ *with* $i_1 > i_2 \ge 1$;

(xviii) $K_n \equiv 26 \pmod{27}$ *if, and only if,* $n = \frac{1}{2}(3^i - 1)$ *with* $i \ge 3$;

(xix) *in the cases not covered by items* (i)–(xvii), K_n *is divisible by* 27; *in particular,* $K_n \not\equiv 4, 10, 11, 13, 19, 20, 22, 25 \pmod{27}$ *for all* n.

Proof. By means of Equation (3.1) and Proposition 9, we convert the right-hand side of (6.6) into a linear combination of series $H_{a_1,a_2,\dots,a_r}\big(z^{1/2}\big)$ with all a_i's relatively prime to p. The result is

$$\begin{aligned}\sum_{n\ge0} K_n\, z^n &= 21z^{-1/2}H_1(z^{1/2}) + 7z^{-1}H_2(z^{1/2}) + 5z^{-1}H_{1,1}(z^{1/2})\\
&\quad + 9z^{-1/2}H_{2,1}(z^{1/2}) + 9z^{-1/2}H_{1,2}(z^{1/2}) + 18z^{-1/2}H_{1,1,1}(z^{1/2})\\
&\quad + 3z^{-1}H_4(z^{1/2}) + 21z^{-1}H_{2,2}(z^{1/2}) + 15z^{-1}H_{2,1,1}(z^{1/2})\\
&\quad + 15z^{-1}H_{1,2,1}(z^{1/2}) + 15z^{-1}H_{1,1,2}(z^{1/2}) + 3z^{-1}H_{1,1,1,1}(z^{1/2})\\
&\quad + 9z^{-1}H_{4,2}(z^{1/2}) + 9z^{-1}H_{2,4}(z^{1/2}) + 18z^{-1}H_{4,1,1}(z^{1/2}) + 18z^{-1}H_{1,4,1}(z^{1/2})\\
&\quad + 18z^{-1}H_{1,1,4}(z^{1/2}) + 9z^{-1}H_{2,2,2}(z^{1/2}) + 18z^{-1}H_{2,2,1,1}(z^{1/2})\\
&\quad + 18z^{-1}H_{2,1,2,1}(z^{1/2}) + 18z^{-1}H_{2,1,1,2}(z^{1/2}) + 18z^{-1}H_{1,2,2,1}(z^{1/2})\\
&\quad + 18z^{-1}H_{1,2,1,2}(z^{1/2}) + 18z^{-1}H_{1,1,2,2}(z^{1/2}) + 9z^{-1}H_{2,1,1,1,1}(z^{1/2})\\
&\quad + 9z^{-1}H_{1,2,1,1,1}(z^{1/2}) + 9z^{-1}H_{1,1,2,1,1}(z^{1/2}) + 9z^{-1}H_{1,1,1,2,1}(z^{1/2})\\
&\quad + 9z^{-1}H_{1,1,1,1,2}(z^{1/2}) + 18z^{-1}H_{1,1,1,1,1,1}(z^{1/2}) \qquad \text{modulo } 27.\end{aligned}$$

Coefficient extraction following the algorithm described in Remark 8 then yields the claimed congruences. □

If we restrict Corollary 17 to modulus 3, then it reduces to the following simple assertion.

Corollary 18. *The number* K_n *of Kreweras walks of length* $3n$ *is congruent to* 1 *modulo* 3 *if, and only if,* $n = 3^i - 1$ *with* $i \ge 1$, *it is congruent to* 2 *modulo* 3 *if, and only if,* $n = \frac{1}{2}(3^{i_1} + 3^{i_2} - 2)$ *with* $i_1 > i_2 \ge 0$, *and it is divisible by* 3 *in all other cases.*

7. Fuss–Catalan numbers modulo p-powers

In this section, given a positive integer h and a prime number p, we determine the behaviour of the *Fuß–Catalan numbers*

$$F(n; k) := \frac{1}{n}\binom{kn}{n-1} \tag{7.1}$$

modulo powers of p, provided k is itself a power of p, say, $k = p^h$.[3] These numbers have numerous combinatorial interpretations; cf. [1, pp. 59–60].

By using the Lagrange inversion formula (see [20, Theorem 5.4.2]), it is easy to see that the generating function $f_{p;h}(z) = 1 + \sum_{n\ge1} \frac{1}{n}\binom{p^h n}{n-1} z^n$ satisfies the functional equation

$$z f_{p;h}^{p^h}(z) - f_{p;h}(z) + 1 = 0. \tag{7.2}$$

It is straightforward to verify that this equation has a unique formal power series solution over $\mathbb{Z}$, and as well over any power of p.

In order to determine the coefficients of $f_{p;h}(z)$ modulo powers of p, we have to use a variant of the series $\Phi(z)$ defined in (1.1), namely

$$\Phi_{p;h}(z) = \sum_{n\ge0} z^{p^{nh}/(p^h-1)}. \tag{7.3}$$

The theorem below generalises Theorem 33 in [12] to arbitrary prime numbers.

Theorem 19. *For a prime number p and a positive integer h, let $\Phi_{p;h}(z)$ be the series defined in* (7.3)*, and let α be a further positive integer. Then the generating function $f_{p;h}(z)$, when reduced modulo p^{p^α}, can be expressed as a polynomial in $\Phi_{p;h}(z)$ of degree at most $p^{(\alpha+1)h} - 1$, with coefficients that are Laurent polynomials in $z^{1/(p^h-1)}$ over the integers.*

Proof. For ease of notation, we replace z by z^{p^h-1} in (7.2), thereby obtaining the equation

$$z^{p^h-1} \tilde f_{p;h}^{p^h}(z) - \tilde f_{p;h}(z) + 1 = 0, \tag{7.4}$$

with $\tilde f_{p;h}(z) = f_{p;h}(z^{p^h-1})$. We now have to prove that, modulo $p^{p^{\alpha h}}$, the series $\tilde f_{p;h}(z)$ can be expressed as a polynomial in

$$\tilde\Phi_{p;h}(z) = \sum_{n=0}^{\infty} z^{p^{nh}} \tag{7.5}$$

of degree at most $p^{(\alpha+1)h} - 1$, with coefficients that are Laurent polynomials in z.

It is readily verified that

$$\tilde\Phi_{p;h}^{p^h}(z) - \tilde\Phi_{p;h}(z) + z = 0 \quad \text{modulo } p, \tag{7.6}$$

whence

$$\left(\tilde\Phi_{p;h}^{p^h}(z) - \tilde\Phi_{p;h}(z) + z\right)^{p^{\alpha h}} = 0 \quad \text{modulo } p^{p^{\alpha h}}. \tag{7.7}$$

We modify our Ansatz (4.2) to

$$\tilde f_{p;h}(z) = \sum_{i=0}^{p^{(\alpha+1)h}-1} a_i(z)\tilde\Phi_{p;h}^i(z) \quad \text{modulo } p^{p^{\alpha h}}, \tag{7.8}$$

where the $a_i(z)$'s are (at this point) undetermined Laurent polynomials in z.

[3] In principle, one could use the generalisations of Lucas' theorem due to Davis and Webb [4], and to Granville [10], respectively, to analyse the explicit expression for the Fuß–Catalan numbers modulo a given p-power. However, this approach would be rather cumbersome in comparison with our method, and it is doubtful that one would be able to derive a result on the same level of generality as Theorems 19, 20, or Corollaries 21, 22.

Next, we gradually find approximations $a_{i,\beta}(z)$ to $a_i(z)$ such that (7.4) holds modulo p^β, for $\beta = 1, 2, \dots, p^{\alpha h}$. To start the procedure, we consider the functional equation (7.4) modulo p, with

$$\tilde{f}_{p;h}(z) = \sum_{i=0}^{p^{(\alpha+1)h}-1} a_{i,1}(z)\tilde{\Phi}^i_{p;h}(z) \quad \text{modulo } p. \tag{7.9}$$

It is readily verified that the choice of

$$a_{0,1}(z) = \sum_{k=0}^{\alpha-1} z^{p^{kh}-1},$$
$$a_{p^{\alpha h},1}(z) = z^{-1}, \tag{7.10}$$

with all other $a_{i,1}(z)$'s equal to zero indeed leads to a solution of (7.4) modulo p.

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. Our Ansatz here (replacing the corresponding one in (4.6)–(4.8)) is

$$\tilde{f}_{p;h}(z) = \sum_{i=0}^{p^{(\alpha+1)h}-1} a_{i,\beta+1}(z)\tilde{\Phi}^i_{p;h}(z) \quad \text{modulo } p^{\beta+1}, \tag{7.11}$$

with

$$a_{i,\beta+1}(z) := a_{i,\beta}(z) + p^\beta b_{i,\beta+1}(z), \quad i = 0, 1, \dots, p^{(\alpha+1)h} - 1, \tag{7.12}$$

where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution

$$\tilde{f}_\beta(z) = \sum_{i=0}^{p^{(\alpha+1)h}-1} a_{i,\beta}(z)\tilde{\Phi}^i_{p;h}(z)$$

to (7.4) modulo p^β. This Ansatz, substituted in (7.4), produces the congruence

$$z^{p^h-1}\tilde{f}_\beta^{p^h}(z) - \tilde{f}_\beta(z) + p^\beta \sum_{i=0}^{p^{(\alpha+1)h}-1} b_{i,\beta+1}(z)\tilde{\Phi}^i_{p;h}(z) + 1 = 0 \quad \text{modulo } p^{\beta+1}. \tag{7.13}$$

By our assumption on $\tilde{f}_\beta(z)$, we may divide by p^β. Comparison of powers of $\tilde{\Phi}_{p;h}(z)$ then yields a system of congruences of the form

$$b_{i,\beta+1}(z) + \mathrm{Pol}_i(z) = 0 \quad \text{modulo } p, \qquad i = 0, 1, \dots, p^{(\alpha+1)h} - 1, \tag{7.14}$$

where $\mathrm{Pol}_i(z)$, $i = 0, 1, \dots, p^{(\alpha+1)h} - 1$, are certain Laurent polynomials with integer coefficients. This system being trivially uniquely solvable, we have proved that, for an arbitrary positive integer α, the modified algorithm that we have presented here will produce a solution $\tilde{f}_{p^{\alpha h}}(z)$ to (7.4) modulo $p^{p^{\alpha h}}$ which is a polynomial in $\tilde{\Phi}_{p;h}(z)$ with coefficients that are Laurent polynomials in$z$. $\square$

It should be observed that the $\alpha = 0$ case of the above proof (see in particular (7.10)) shows that $F(n; p^h) \equiv 1 \pmod p$ for $n = (p^{hi} - 1)/(p - 1)$, $i = 0, 1, \dots,$ and $F(n; p^h) \equiv 0 \pmod p$ otherwise.

We have implemented the algorithm contained in the above proof. As an illustration, we display below the result obtained for $h = 1$ and the modulus p^2. This result was first guessed from the automatically obtained results for $p = 3, 5, 7$, but, once found, it is easily verified directly by substitution in (7.2).

Theorem 20. *Let $\Phi(z) = \sum_{n\ge0} z^{p^n}$. Then we have*

$$\sum_{n\ge1} \frac{1}{n}\binom{pn}{n-1} z^n = p\Phi^{p-1}\big(z^{1/(p-1)}\big) - (p-1)z^{-1/(p-1)}\Phi^p\big(z^{1/(p-1)}\big) + pz^{-1/(p-1)}\Phi^{2p-1}\big(z^{1/(p-1)}\big) \qquad \text{modulo } p^2. \quad (7.15)$$

(Human) inspection reveals that this expression can actually be drastically simplified.

Corollary 21. *Let $\Phi(z) = \sum_{n\ge0} z^{p^n}$. Then we have*

$$\sum_{n\ge1} \frac{1}{n}\binom{pn}{n-1} z^n = z^{-1/(p-1)}\Phi^p\big(z^{1/(p-1)}\big) \qquad \text{modulo } p^2. \qquad (7.16)$$

Proof. One applies relation (4.4) with $\alpha = 0$ and z replaced by $z^{1/(p-1)}$ to the terms in (7.15) which have coefficient p. $\square$

Explicitly, this leads to the following congruences modulo p^2.

Corollary 22. *The Fuß–Catalan numbers $F(n;p) = \frac{1}{n}\binom{pn}{n-1}$ obey the following congruences modulo p^2:*

(i) *If $n = \frac{1}{p-1}(p^i - 1)$ with $i \ge 1$, then $F(n;p) \equiv 1 \pmod{p^2}$.*

(ii) *If*

$$n = \frac{1}{p-1}\left(a_1 p^{i_1} + a_2 p^{i_2} + \cdots + a_r p^{i_r} - 1\right)$$

with all a_i's relatively prime to p, $a_1 + a_2 + \cdots + a_r = p$, $r \ge 2$, and $i_1 > i_2 > \cdots > i_r \ge 0$, then we have

$$F(n;p) \equiv \frac{p!}{a_1!\,a_2!\cdots a_r!} \pmod{p^2}.$$

(iii) *In the cases not covered by items* (i) *and* (ii), *the Fuß–Catalan number $F(n;p)$ is divisible by p^2.*

Proof. By means of Equation (3.1) and Proposition 9, we convert the right-hand side of (5.8) into a linear combination of series $H_{a_1,a_2,\dots,a_r}\big(z^{1/(p-1)}\big)$, with all a_i's relatively prime to p. The result is

$$\sum_{n\ge1} \frac{1}{n}\binom{pn}{n-1} z^n = z^{-1/(p-1)}H_1\big(z^{1/(p-1)}\big) - 1 + z^{-1/(p-1)}\sum_{r=1}^{p}\sum_{\substack{a_1,\dots,a_r\ge1\\ a_1+\cdots+a_r=p \text{ and } r\ge2}} \frac{p!}{a_1!\,a_2!\cdots a_r!}H_{a_1,a_2,\dots,a_r}\big(z^{1/(p-1)}\big) \qquad \text{modulo } p^2.$$

Coefficient extraction then leads to our claim. $\square$

8. The number of blossom trees modulo p-powers

The combinatorial objects which we treat in this section are so-called "blossom trees." These are a particular kind of trees which are of great significance in the combinatorial understanding of the enumeration of maps; see e.g. the survey [3]. The particular blossom trees that we are interested in are the ones in [18, Sec. 3]. Since the precise definition is slightly technical and not needed here, we omit it, and instead refer the reader to [18].

For an odd positive integer k, let $B(n;k)$ be the number of blossom trees constructed from k-ary trees with n white nodes by adding a black node with $k-1$ buds on each inner edge. Let $B_k(z) := \frac{k+1}{2} + \sum_{n\ge1} B(n;k)\,z^n$ be the corresponding generating function. Schaeffer [18, Cor. 2] proved that

$$B(n;k) = \frac{k+1}{n((k-1)n+2)}\binom{kn}{n-1}. \tag{8.1}$$

As we show in the Appendix, the generating function $B_k(z)$ satisfies the polynomial equation

$$z^2B_k^k(z) + \sum_{s=0}^{(k+1)/2}(-1)^s\frac{k+1}{(k-s+1)(k-s)}\binom{k-s+1}{s}k^{k-2s+1}\left(\frac{k-1}{2}\right)^s zB_k^s(z) \\ -(-1)^k\left(\frac{k-1}{2}\right)^{k-1}B_k(z) + (-1)^k\frac{k+1}{2}\left(\frac{k-1}{2}\right)^{k-1} = 0. \tag{8.2}$$

It is not difficult to see that (8.2) determines $B_k(z)$ uniquely as a formal power series over $\mathbb{Z}$, and as well over any power of a prime number p as long as $k \not\equiv 1 \pmod p$.

From now on, let p be a fixed odd prime number.

Theorem 23. *Let $\Phi(z) = \sum_{n\ge0} z^{p^n}$, and let α be a non-negative integer. Then the generating function $B_p(z)$, when reduced modulo p^{p^α}, can be expressed as a polynomial in $\Phi\left(z^{1/(p-1)}\right)$ of degree at most $p^{\alpha+1}-1$, with coefficients that are Laurent polynomials in $z^{1/(p-1)}$ over the integers.*

Proof. Again, we apply the method from Section 4. To begin with, we need a "base solution"

$$F_1(z) = \sum_{i=0}^{p^{\alpha+1}-1} a_{i,1}(z)\Phi^i\left(z^{1/(p-1)}\right) \tag{8.3}$$

to (8.2) modulo p. At this point, it is useful to observe that, using Fermat's little theorem, the functional equation (8.2), when taken modulo p, reduces to

$$z^2B_p^p(z) - 2^{(p+1)/2}zB_p^{(p+1)/2}(z) + B_p(z) - 2^{-1} = 0 \quad \text{modulo } p, \tag{8.4}$$

where here, and in the following, 2^{-1} denotes the inverse of 2 modulo p. We claim that the following choices in (8.3) solve the above congruence:

$$a_{0,1}(z) = 2^{-1}z^{-2/(p-1)}s_\alpha^2(z^{1/(p-1)}) \quad \text{modulo } p,$$

$$a_{p^\alpha,1}(z) = z^{-2/(p-1)}s_\alpha(z^{1/(p-1)}) \quad \text{modulo } p,$$

$$a_{2\cdot p^\alpha,1}(z) = 2^{-1}z^{-2/(p-1)} \quad \text{modulo } p,$$

where $s_\alpha(z)=\sum_{k=0}^{\alpha-1} z^{p^k}$, with all other $a_{i,1}(z)$ vanishing. In order to verify this claim, we first observe that, with the above choices, $F_1(z)$ can be expressed as a square, namely

$$F_1(z)=2^{-1}z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^2.$$

We substitute this in (8.4). For the left-hand side, we obtain

$$\begin{aligned}2^{-1}z^{-2/(p-1)}&\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^{2p}\\ &-z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^{p+1}\\ &+2^{-1}z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^{2}-2^{-1}\quad\text{modulo } p.\end{aligned}$$

Using the relation (4.5) with z replaced by $z^{1/(p-1)}$ and reducing the obtained expression modulo p, we arrive at

$$\begin{aligned}&2^{-1}z^{-2/(p-1)}\left(\Phi^{p^{\alpha+1}}\big(z^{1/(p-1)}\big)+s_\alpha^p\big(z^{1/(p-1)}\big)\right)^2\\
&\quad-z^{-2/(p-1)}\left(\Phi^{p^{\alpha+1}}\big(z^{1/(p-1)}\big)+s_\alpha^p\big(z^{1/(p-1)}\big)\right)\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)\\
&\quad+2^{-1}z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^2-2^{-1}\\
&=2^{-1}z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)-z^{p^\alpha/(p-1)}+s_{\alpha+1}\big(z^{1/(p-1)}\big)-z^{1/(p-1)}\right)^2\\
&\quad-z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)-z^{p^\alpha/(p-1)}+s_{\alpha+1}\big(z^{1/(p-1)}\big)-z^{1/(p-1)}\right)\\
&\qquad\qquad\times\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)\\
&\quad+2^{-1}z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^2-2^{-1}\\
&=2^{-1}z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)-z^{1/(p-1)}\right)^2\\
&\quad-z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)-z^{1/(p-1)}\right)\\
&\qquad\qquad\times\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)\\
&\quad+2^{-1}z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^2-2^{-1}\quad\text{modulo } p.\end{aligned}$$

By collecting terms, this expression may be simplified to zero.

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. Our Ansatz here (replacing the corresponding one in (4.6)–(4.8)) is

$$B_p(z)=\sum_{i=0}^{p^{(\alpha+1)h}-1}a_{i,\beta+1}(z)\Phi^i\left(z^{1/(p-1)}\right)\quad\text{modulo } p^{\beta+1},\tag{8.5}$$

with

$$a_{i,\beta+1}(z):=a_{i,\beta}(z)+p^\beta b_{i,\beta+1}(z),\quad i=0,1,\dots,p^{(\alpha+1)h}-1,\tag{8.6}$$

where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution

$$F_\beta(z)=\sum_{i=0}^{p^{(\alpha+1)h}-1}a_{i,\beta}(z)\Phi^i\left(z^{1/(p-1)}\right)$$

to (8.2) modulo p^β. This Ansatz, substituted in (8.2), produces the congruence

$$\begin{aligned}
2(-1)^{(p+1)/2}\left(\frac{p-1}{2}\right)^{(p-1)/2}\frac{p+1}{2}&\\
\times p^\beta z\left(\sum_{i=0}^{p^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^i\big(z^{1/(p-1)}\big)\right)&\left(\sum_{j=0}^{p^{\alpha+1}-1} a_{j,\beta}(z)\Phi^j\big(z^{1/(p-1)}\big)\right)^{(p-1)/2}\\
+\left(\frac{p-1}{2}\right)^{p-1}p^\beta\left(\sum_{i=0}^{p^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^i\big(z^{1/(p-1)}\big)\right)&\\
+z^2F_\beta^p(z)+\sum_{s=0}^{(p+1)/2}(-1)^s\frac{p+1}{(p-s+1)(p-s)}\binom{p-s+1}{s}&p^{p-2s+1}\left(\frac{p-1}{2}\right)^s zF_\beta^s(z)\\
+\left(\frac{p-1}{2}\right)^{p-1}F_\beta(z)-\frac{p+1}{2}\left(\frac{p-1}{2}\right)^{p-1}&=0\qquad\text{modulo } p^{\beta+1}.
\end{aligned}\tag{8.7}$$

Since the sum has the prefactor p^β, we may reduce the $a_{i,\beta}(z)$ modulo p. By construction, we have

$$\begin{aligned}
a_{0,\beta}(z)=a_{0,1}(z)&=2^{-1}z^{-2/(p-1)}s_\alpha^2\big(z^{1/(p-1)}\big)\qquad\text{modulo } p,\\
a_{p^\alpha,\beta}(z)=a_{p^\alpha,1}(z)&=z^{-2/(p-1)}s_\alpha\big(z^{1/(p-1)}\big)\qquad\text{modulo } p,\\
a_{2\cdot p^\alpha,\beta}(z)=a_{2\cdot p^\alpha,1}(z)&=2^{-1}z^{-2/(p-1)}\qquad\text{modulo } p,
\end{aligned}$$

and $a_{i,\beta}=0$ modulo p for all other i's. Equivalently, we have

$$F_\beta(z)=2^{-1}z^{-2/(p-1)}\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^2\qquad\text{modulo } p.$$

If we substitute this in (8.7) and divide both sides of the congruence by p^β (which is possible by our assumption on $F_\beta(z)$), we obtain

$$\begin{aligned}
-\left(\sum_{i=0}^{p^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^i\big(z^{1/(p-1)}\big)\right)&\left(\Phi^{p^\alpha}\big(z^{1/(p-1)}\big)+s_\alpha\big(z^{1/(p-1)}\big)\right)^{p-1}\\
&+\left(\sum_{i=0}^{p^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^i\big(z^{1/(p-1)}\big)\right)+G_\beta(z)\\
=-\left(\sum_{i=0}^{p^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^i\big(z^{1/(p-1)}\big)\right)&\left(\sum_{j=0}^{p-1}(-1)^j\Phi^{jp^\alpha}\big(z^{1/(p-1)}\big)\,s_\alpha^{p-j-1}\big(z^{1/(p-1)}\big)\right)\\
&+\left(\sum_{i=0}^{p^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^i\big(z^{1/(p-1)}\big)\right)+G_\beta(z)=0\qquad\text{modulo } p,
\end{aligned}$$

where $G_\beta(z)$ is some polynomial in $\Phi\left(z^{1/(p-1)}\right)$ whose coefficients are Laurent polynomials in $z^{1/(p-1)}$ with integer coefficients. Upon using (4.5) with z replaced by $z^{1/(p-1)}$

to reduce high powers of $\Phi\big(z^{1/(p-1)}\big)$, we convert this congruence into

$$
\begin{aligned}
-\sum_{j=0}^{p-1}\sum_{i=jp^\alpha}^{p^{\alpha+1}-1} \Phi^i\big(z^{1/(p-1)}\big)\,(-1)^j b_{i-jp^\alpha,\beta+1}(z) s_\alpha^{p-j-1}\big(z^{1/(p-1)}\big)&\\
-\sum_{j=0}^{p-1}\sum_{i=p^\alpha}^{(j+1)p^\alpha-1} \Phi^i\big(z^{1/(p-1)}\big)\,(-1)^j b_{i+(p-j-1)p^\alpha,\beta+1}(z) s_\alpha^{p-j-1}\big(z^{1/(p-1)}\big)&\\
+\sum_{j=0}^{p-1}\sum_{i=0}^{jp^\alpha-1} \Phi^i\big(z^{1/(p-1)}\big)\,(-1)^j z^{p^\alpha/(p-1)} b_{i+(p-j)p^\alpha,\beta+1}(z) s_\alpha^{p-j-1}\big(z^{1/(p-1)}\big)&\\
+\left(\sum_{i=0}^{p^{\alpha+1}-1} b_{i,\beta+1}(z)\Phi^i\big(z^{1/(p-1)}\big)\right)+G_\beta(z)=0 \qquad \text{modulo } p,&
\end{aligned}
$$

Comparison of powers of $\Phi(z)$ then yields a system of congruences of the form

$$M\cdot b = c \quad \text{modulo } p, \tag{8.8}$$

where b is the column vector of unknowns $(b_{i,\beta+1}(z))_{i=0,1,\dots,p^{\alpha+1}-1}$, c is a (known) column vector of Laurent polynomials in z, and M is the matrix

$$
\begin{pmatrix}
D(1-s_\alpha^{p-1}) & D(z^A) & D(-z^A s_\alpha) & \dots & D(z^A s_\alpha^{p-3}) & D(-z^A s_\alpha^{p-2})\\
D(s_\alpha^{p-2}) & D(-s_\alpha^{p-1}) & D(s_\alpha+z^A) & \dots & D(-s_\alpha^{p-3}-z^A s_\alpha^{p-4}) & D(s_\alpha^{p-2}+z^A s_\alpha^{p-3})\\
D(-s_\alpha^{p-3}) & D(s_\alpha^{p-2}) & D(-s_\alpha^{p-1}) & \dots & D(s_\alpha^{p-4}+z^A s_\alpha^{p-5}) & D(-s_\alpha^{p-3}-z^A s_\alpha^{p-4})\\
\vdots & \vdots & \vdots & \ddots & & \\
D(s_\alpha) & D(-s_\alpha^2) & D(s_\alpha^3) & \dots & D(-s_\alpha^{p-1}) & D(s_\alpha+z^A)\\
D(-1) & D(s_\alpha) & D(-s_\alpha^2) & \dots & D(s_\alpha^{p-2}) & D(-s_\alpha^{p-1})
\end{pmatrix},
$$

where s_α is short for $s_\alpha\big(z^{1/(p-1)}\big)$, A is short for $p^\alpha/(p-1)$, and $D(x)$ denotes the $p^\alpha\times p^\alpha$ diagonal matrix whose diagonal entries equal x. More precisely, the (r,t)-block of the matrix, $0\le r,t\le p-1$, is given by

$$
\begin{cases}
D(1-s_\alpha^{p-1}), & \text{if } r=t=0,\\
D((-1)^{t-1}z^A s_\alpha^{t-1}), & \text{if } r=0 \text{ and } t>0,\\
D((-1)^{r-t+1}s_\alpha^{p-1-r+t}), & \text{if } r\ge t \text{ but not } r=t=0,\\
D((-1)^{t-r-1}s_\alpha^{t-r-1}(s_\alpha+z^A)), & \text{if } 0<r<t.
\end{cases}
$$

We claim that

$$\det(M)=z^{p^\alpha} \qquad \text{modulo } p.$$

In order to see this, we add $1-s_\alpha^{p-1}(z)$ times row $i+(p-1)\cdot p^\alpha$ to row i, $i=0,1,\dots,p^\alpha-1$, and we add $s_\alpha\big(z^{1/(p-1)}\big)$ times row $i+p^\alpha$ to row i, $i=p^\alpha,p^\alpha+1,\dots,p^{\alpha+1}-1$. This leads to the matrix

$$
\begin{pmatrix}
0 & D(s_\alpha+z^A-s_\alpha^p) & * & \dots & * & *\\
0 & 0 & D(s_\alpha+z^A-s_\alpha^p) & \dots & 0 & 0\\
0 & 0 & 0 & \dots & 0 & 0\\
\vdots & \vdots & \vdots & \ddots & & \\
0 & 0 & 0 & \dots & 0 & D(s_\alpha+z^A-s_\alpha^p)\\
D(-1) & D(s_\alpha) & D(-s_\alpha^2) & \dots & D(s_\alpha^{p-2}) & D(-s_\alpha^{p-1})
\end{pmatrix}.
$$

If, in addition, we move rows $(p-1)\cdot p^\alpha, (p-1)\cdot p^\alpha+1,\dots,p^{\alpha+1}-1$ to the top of the matrix, then it attains an upper triangular form, from which one infers that

$$\begin{aligned}\det(M)&=(-1)^{(p-1)\cdot p^\alpha\cdot p^\alpha}\det{}^{p-1}\Big(D\big(s_\alpha\big(z^{1/(p-1)}\big)+z^{p^\alpha/(p-1)}-s_\alpha^p\big(z^{1/(p-1)}\big)\big)\Big)\det\big(D(1)\big)\\&=\Big(s_\alpha\big(z^{1/(p-1)}\big)+z^{p^\alpha/(p-1)}-s_\alpha^p\big(z^{1/(p-1)}\big)\Big)^{(p-1)\cdot p^\alpha}\\&=z^{p^\alpha}\qquad\text{modulo } p,\end{aligned}$$

as was claimed. As a consequence, the system (8.8) is (uniquely) solvable. Thus, we have proved that, for an arbitrary non-negative integer α, the algorithm of Section 4 will produce a solution $F_{p^\alpha}(z)$ to (8.2) modulo p^{p^α} which is a polynomial in $\Phi\big(z^{1/(p-1)}\big)$ with coefficients that are Laurent polynomials in z. $\square$

A direct corollary of the $\alpha=0$ case of the preceding proof is the following.

Corollary 24. *The blossom tree numbers $B(n;p)=\frac{k+1}{n((p-1)n+2)}\binom{pn}{n-1}$ obey the following congruences modulo p:*

(i) *If $n=\frac{1}{p-1}(p^{i_1}+p^{i_2}-2)$ with $i_1-1>i_2\ge 0$, then $B(n;p)\equiv 1 \pmod p$.*
(ii) *If $n=\frac{1}{p-1}(2p^i-2)$ with $i\ge 1$, then $B(n;p)\equiv\frac{p+1}{2}\pmod p$.*
(iii) *In the cases not covered by items* (i) *and* (ii), *the number $B(n;p)$ is divisible by p.*

Obviously, one can do better by using an implementation of the algorithm contained in the proof of Theorem 23. As an illustration, we display below the result obtained for the modulus p^2. Again, this result was first guessed from the automatically obtained results for $p=3,5,7$, but, once found, it is easily verified directly by substitution in (8.4).

Theorem 25. *Let $\Phi(z)=\sum_{n\ge 0} z^{p^n}$. Then we have*

$$\begin{aligned}\frac{p+1}{2}+\sum_{n\ge 1}B(n;p)\,z^n=(p+1)z^{-1/(p-1)}\Phi\big(z^{1/(p-1)}\big)-\frac{p+1}{2}z^{-2/(p-1)}\Phi^2\big(z^{1/(p-1)}\big)\\+z^{-2/(p-1)}\Phi^{p+1}\big(z^{1/(p-1)}\big)\qquad\text{modulo } p^2.\end{aligned}\tag{8.9}$$

Explicitly, this means the following.

Corollary 26. *The blossom tree numbers $B(n;p)=\frac{k+1}{n((p-1)n+2)}\binom{pn}{n-1}$ obey the following congruences modulo p^2:*

(i) *If $n=\frac{1}{p-1}((p+1)p^i-2)$ with $i\ge 0$, then $B(n;p)\equiv 1 \pmod{p^2}$.*
(ii) *If $n=\frac{1}{p-1}(2p^i-2)$ with $i\ge 1$, then $B(n;p)\equiv\frac{p+1}{2}\pmod{p^2}$.*
(iii) *If $n=\frac{1}{p-1}(p^{i_1}+p^{i_2}-2)$ with $i_1-1>i_2\ge 0$, then $B(n;p)\equiv p+1\pmod{p^2}$.*
(iv) *If*

$$n=\frac{1}{p-1}\left(a_1p^{i_1}+a_2p^{i_2}+\cdots+a_rp^{i_r}-2\right)$$

with all a_i's relatively prime to p, $a_1+a_2+\cdots+a_r=p+1$, $r\ge 2$, and $i_1>i_2>\cdots>i_r\ge 0$, then we have

$$B(n;p)\equiv\frac{(p+1)!}{a_1!\,a_2!\cdots a_r!}\pmod{p^2}.$$

(v) *In the cases not covered by items* (i)–(iv), *the number $B(n;p)$ is divisible by p^2.*

Proof. By means of Equation (3.1) and Proposition 9, we convert the right-hand side of (8.9) into a linear combination of series $H_{a_1,a_2,\dots,a_r}\big(z^{1/(p-1)}\big)$ with all a_i's relatively prime to p. The result is

$$\begin{aligned}\sum_{n\ge0} B(n;p)\,z^n &= \frac{p+1}{2} z^{-2/(p-1)} H_2\big(z^{1/(p-1)}\big) + (p+1) z^{-2/(p-1)} H_{1,1}\big(z^{1/(p-1)}\big)\\ &\qquad - p z^{-2/(p-1)} H_{p+1}\big(z^{1/(p-1)}\big)\\ &+ z^{-2/(p-1)} \sum_{r=1}^{p+1} \sum_{\substack{a_1,\dots,a_r\ge1\\ a_1+\dots+a_r=p+1\\ r\ge2 \text{ and } a_i\ne p \text{ for all } i}} \frac{(p+1)!}{a_1!\,a_2!\cdots a_r!} H_{a_1,a_2,\dots,a_r}\big(z^{1/(p-1)}\big) \qquad \text{modulo } p^2.\end{aligned}$$

Coefficient extraction then yields the claimed congruences. $\square$

Appendix: Proof of the functional equation (8.2)

Let k be a positive integer and let

$$T_k(z) = \sum_{n\ge1} \frac{1}{n} \binom{kn}{n-1} z^n$$

be the generating function for the general Fuß–Catalan numbers. We claim that the blossom tree generating function $B_k(z)$ can be expressed in terms of $T_k(z)$ as follows.

Lemma 27. *For all positive integers k, we have*

$$B_k(z) = (1+T_k(z))\left(k - \frac{k-1}{2}(1+T_k(z))\right). \tag{A.1}$$

Proof. We verify that the coefficient of z^n is the same on both sides of (A.1), for $n = 0, 1, \dots$ Clearly, the constant coefficient equals $(k+1)/2$ on both sides.

Now let $n \ge 1$. It is easily seen by Lagrange inversion (see [20, Theorem 5.4.2]), that the series $T_k(z)$ satisfies the equation

$$T_k(z) = z(1+T_k(z))^k. \tag{A.2}$$

In other words, it is the compositional inverse of $z/(1+z)^k$. By applying Lagrange inversion again, we infer

$$\begin{aligned}\langle z^n\rangle (1+T_k(z))\left(k - \frac{k-1}{2}(1+T_k(z))\right) &= \frac{1}{n}\left\langle z^{-1}\right\rangle (1-(k-1)z)\,\frac{(1+z)^{kn}}{z^n}\\ &= \frac{1}{n}\left(\left\langle z^{n-1}\right\rangle (1+z)^{kn} - (k-1)\left\langle z^{n-2}\right\rangle (1+z)^{kn}\right)\\ &= \frac{1}{n}\left(\binom{kn}{n-1} - (k-1)\binom{kn}{n-2}\right)\\ &= \frac{k+1}{n((k-1)n+2)}\binom{kn}{n-1} = B(n;k).\end{aligned}$$

$\square$

Proof of (8.2). In order to establish (8.2), we substitute the right-hand side of (A.1) for $B_k(z)$ in (8.2). After applying the binomial theorem, we obtain

$$
\begin{aligned}
&z^2\sum_{j=0}^{k}(-1)^j\binom{k}{j}k^{k-j}\left(\frac{k-1}{2}\right)^j X(z)^{k+j}\\
&\qquad+\sum_{s=0}^{(k+1)/2}\sum_{j=0}^{s}(-1)^{s+j}\frac{k+1}{(k-s+1)(k-s)}\\
&\qquad\qquad\qquad\cdot\binom{k-s+1}{s}\binom{s}{j}k^{k-s-j+1}\left(\frac{k-1}{2}\right)^{s+j} zX(z)^{s+j}\\
&\qquad\quad-(-1)^k\left(\frac{k-1}{2}\right)^{k-1}X(z)\left(k-\frac{k-1}{2}X(z)\right)+(-1)^k\frac{k+1}{2}\left(\frac{k-1}{2}\right)^{k-1}
\end{aligned}
$$

on the left-hand side, where $X(z)=1+T_k(z)$. In order to simplify, we use the relation (A.2) in the first term, we replace s by $s-j$, and then write the sum over j in standard hypergeometric notation

$$
{}_pF_q\left[\begin{matrix}a_1,\dots,a_p\\ b_1,\dots,b_q\end{matrix};z\right]=\sum_{m=0}^{\infty}\frac{(a_1)_m\cdots(a_p)_m}{m!\,(b_1)_m\cdots(b_q)_m}z^m\ ,
$$

where the Pochhammer symbol $(\alpha)_m$ is defined by $(\alpha)_m:=\alpha(\alpha+1)\cdots(\alpha+m-1)$, $m\ge 1$, and $(\alpha)_0:=1$. In this manner, we arrive at

$$
\begin{aligned}
&z\sum_{j=0}^{k}(-1)^j\binom{k}{j}k^{k-j}\left(\frac{k-1}{2}\right)^j(X(z)-1)X(z)^j\\
&\qquad+2(-1)^{k+1}\left(\frac{k-1}{2}\right)^k zX(z)^{k+1}+(-1)^k k(k+1)\left(\frac{k-1}{2}\right)^{k-1}zX(z)^k\\
&\qquad+\sum_{s=0}^{k-1}(-1)^s\frac{(k+1)\,(k-s-1)!}{(k-2s+1)!\,s!}k^{k-s+1}\left(\frac{k-1}{2}\right)^s\\
&\qquad\qquad\qquad\cdot zX(z)^s\,{}_3F_2\left[\begin{matrix}k-s,-\frac{s}{2},-\frac{s}{2}+1\\ \frac{k}{2}-s+\frac{1}{2},\frac{k}{2}-s+1\end{matrix};1\right]\\
&\qquad\quad-(-1)^k\left(\frac{k-1}{2}\right)^{k-1}X(z)\left(k-\frac{k-1}{2}X(z)\right)+(-1)^k\frac{k+1}{2}\left(\frac{k-1}{2}\right)^{k-1}
\end{aligned}
$$

The ${}_3F_2$-series can be evaluated by means of the Pfaff–Saalschütz summation formula (see [19, (2.3.1.3), Appendix (III.2)])

$$
{}_3F_2\left[\begin{matrix}a,b,-n\\ c,1+a+b-c-n\end{matrix};1\right]=\frac{(c-a)_n\,(c-b)_n}{(c)_n\,(c-a-b)_n},
$$

provided n is a non-negative integer. Thus, we obtain

$$\sum_{j=0}^{k}(-1)^j\binom{k}{j}k^{k-j}\left(\frac{k-1}{2}\right)^j z(X(z)-1)X(z)^j$$
$$+2(-1)^{k+1}\left(\frac{k-1}{2}\right)^k zX(z)^{k+1}+(-1)^k k(k+1)\left(\frac{k-1}{2}\right)^{k-1} zX(z)^k$$
$$+\sum_{s=0}^{k-1}(-1)^s\frac{(k+s-1)}{2}k^{k-s}\left(\frac{k-1}{2}\right)^{s-1}\binom{k+1}{s}zX(z)^s$$
$$-(-1)^k\left(\frac{k-1}{2}\right)^{k-1}X(z)\left(k-\frac{k-1}{2}X(z)\right)+(-1)^k\frac{k+1}{2}\left(\frac{k-1}{2}\right)^{k-1}$$
$$=\sum_{j=0}^{k}(-1)^j\binom{k}{j}k^{k-j}\left(\frac{k-1}{2}\right)^j z(X(z)-1)X(z)^j$$
$$+(-1)^{k+1}\left(\frac{k-1}{2}\right)^k zX(z)^{k+1}+(-1)^k\frac{k+1}{2}\left(\frac{k-1}{2}\right)^{k-1} zX(z)^k$$
$$+\sum_{s=0}^{k+1}(-1)^s\frac{(k+s-1)}{2}k^{k-s}\left(\frac{k-1}{2}\right)^{s-1}\binom{k+1}{s}zX(z)^s$$
$$-(-1)^k\left(\frac{k-1}{2}\right)^{k-1}X(z)\left(k-\frac{k-1}{2}X(z)\right)+(-1)^k\frac{k+1}{2}\left(\frac{k-1}{2}\right)^{k-1}.$$

In the last expression, the sums can in fact be extended to run over *all* integers j respectively s. A comparison of powers of $X(z)$ then makes it obvious that the sum over j cancels with the sum over s. To the remaining terms $X^{k+1}(z)$ and $X^k(z)$ we apply again the relation (A.2). This turns the above expression into

$$(-1)^{k+1}\left(\frac{k-1}{2}\right)^k(X(z)-1)X(z)+(-1)^k\frac{k+1}{2}\left(\frac{k-1}{2}\right)^{k-1}(X(z)-1)$$
$$-(-1)^k\left(\frac{k-1}{2}\right)^{k-1}X(z)\left(k-\frac{k-1}{2}X(z)\right)+(-1)^k\frac{k+1}{2}\left(\frac{k-1}{2}\right)^{k-1}=0,$$

which finishes the proof of (8.2). □

References

[1] D. Armstrong, *Generalized noncrossing partitions and combinatorics of Coxeter groups*, Mem. Amer. Math. Soc., vol. 202, no. 949, Amer. Math. Soc., Providence, R.I., 2009.

[2] M. Bousquet–Mélou, Walks in the quarter plane — Kreweras' algebraic model, *Ann. Appl. Probab.* **15** (2005), 1451–1491.

[3] M. Bousquet–Mélou, Counting planar maps, coloured or uncoloured, in: Surveys in Combinatorics 2011, London Math. Soc. Lecture Note Ser., vol. 392, Cambridge Univ. Press, Cambridge, 2011, pp. 1–49.

[4] K. S. Davis and W. A. Webb, Lucas' theorem for prime powers, Europ. J. Combin. **11** (1990), 229–233.

[5] E. Deutsch and B. E. Sagan, Congruences for Catalan and Motzkin numbers and related sequences, *J. Number Theory* **117** (2006), 191–215.

[6] C. Domb and A. Barrett, Enumeration of ladder graphs, *Discrete Math.* **9** (1974), 341–358.

[7] S.-P. Eu, S.-C. Liu, and Y.-N. Yeh, On the congruences of some combinatorial numbers, *Stud. Appl. Math.* **116** (2006), 135–144.
[8] P. Flajolet and M. Noy, Analytic combinatorics of non-crossing configurations, *Discrete Math.* **204** (1999), 203–229.
[9] I. M. Gessel, A short proof of the Deutsch–Sagan congruence for connected noncrossing graphs, preprint; arχiv:1403.7656.
[10] A. Granville, Arithmetic properties of binomial coefficients, I: Binomial coefficients modulo prime powers, in: Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253–276.
[11] Q.-H. Hou, Comment on paper P37 of volume 18(2), *Electron. J. Combin.*, 2012.
[12] M. Kauers, C. Krattenthaler, and T. W. Müller, A method for determining the mod-2^k behaviour of recursive sequences, with applications to subgroup counting, *Electron. J. Combin.* **18**(2) (2012), Article P37, 83 pp.
[13] C. Krattenthaler and T. W. Müller, A method for determining the mod-3^k behaviour of recursive sequences, preprint; arχiv:1308.2856.
[14] G. Kreweras, Sur une classe de problèmes de dénombrement liés au treillis des partitions des entiers, *Cahiers du B.U.R.O. Univ. de Rech. Opér.*, **6** (1965), 5–105.
[15] A. M. Legendre, *Essai sur la théorie des nombres*, 2ed., Courcier, Paris, 1808.
[16] H. Niederhausen, The ballot problem with three candidates, *Europ. J. Combin.* **4** (1983), 161–167.
[17] E. Rowland and R. Yassawi, Automatic congruences for diagonals of rational functions, *J. Théorie Nombres Bordeaux* **27** (2015), 245–288.
[18] G. Schaeffer, A combinatorial interpretation of super-Catalan numbers of order two, unpublished manuscript, 2003; available at http://www.lix.polytechnique.fr/Labo/Gilles.Schaeffer/Biblio/Sc03.ps.
[19] L. J. Slater, *Generalized hypergeometric functions*, Cambridge University Press, Cambridge, 1966.
[20] R. P. Stanley, *Enumerative Combinatorics*, vol. 2, Cambridge University Press, Cambridge, 1999.

†Fakultät für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, A-1090 Vienna, Austria. WWW: http://www.mat.univie.ac.at/~kratt.

*School of Mathematical Sciences, Queen Mary & Westfield College, University of London, Mile End Road, London E1 4NS, United Kingdom.