FROM GENERATING SERIES TO POLYNOMIAL CONGRUENCES

SANDRO MATTAREI AND ROBERTO TAURASO

Abstract. Consider an ordinary generating function $\sum_{k=0}^{\infty} c_k x^k$, of an integer sequence of some combinatorial relevance, and assume that it admits a closed form $C(x)$. Various instances are known where the corresponding truncated sum $\sum_{k=0}^{q-1} c_k x^k$, with q a power of a prime p, also admits a closed form representation when viewed modulo p. Such a representation for the truncated sum modulo p frequently bears a resemblance with the shape of $C(x)$, despite being typically proved through independent arguments. One of the simplest examples is the congruence $\sum_{k=0}^{q-1} \binom{2k}{k} x^k \equiv (1-4x)^{(q-1)/2} \pmod{p}$ being a finite match for the well-known generating function $\sum_{k=0}^{\infty} \binom{2k}{k} x^k = 1/\sqrt{1-4x}$.

We develop a method which allows one to directly infer the closed-form representation of the truncated sum from the closed form of the series for a significant class of series involving central binomial coefficients. In particular, we collect various known such series whose closed-form representation involves polylogarithms $\mathrm{Li}_d(x) = \sum_{k=1}^{\infty} x^k/k^d$, and after supplementing them with some new ones we obtain closed-forms modulo p for the corresponding truncated sums, in terms of finite polylogarithms $\pounds_d(x) = \sum_{k=1}^{p-1} x^k/k^d$.

1. Introduction

There is a vast and expanding literature on evaluating sums of combinatorial numbers such as binomial coefficients modulo a prime p, or a power of a prime. Among the simplest examples are

$$(1) \qquad \sum_{k=0}^{q-1} \binom{2k}{k} \equiv \left(\frac{q}{3}\right) \pmod{p}, \quad \text{and} \quad \sum_{k=0}^{q-1} C_k \equiv \frac{3\left(\frac{q}{3}\right)-1}{2} \pmod{p},$$

where q is a power of a prime p,

$$C_k = \frac{1}{k+1}\binom{2k}{k} = \binom{2k}{k} - \binom{2k}{k+1}$$

denotes the kth *Catalan number*, and $\left(\frac{a}{3}\right)$ is a Legendre symbol. More general forms of congruences (1), and variations, were established in [11, Theorem 1.2 and Corollary 1.3], and later extended in various directions by several authors, see for example [12, Theorem 1.1], but in this Introduction we take the simple formulations in Equations (1) to illustrate the general principle which informs this paper.

2010 *Mathematics Subject Classification.* Primary 11A07; secondary 05A10, 11B83.

Key words and phrases. congruences; binomial coefficients; harmonic numbers; polylogarithms; generating functions.

Many such congruences happen to be specializations of more general polynomial congruences, such as

$$\sum_{k=0}^{q-1} \binom{2k}{k} x^k \equiv (1-4x)^{(q-1)/2} \pmod{p} \tag{2}$$

in case of the former of Equations (1), see Theorem 2 below, which can then easily be recovered by specializing at $x = 1$. Such polynomial formulations, when they exist, are manifestly superior to their numerical counterparts for other reasons beyond allowing specialization at any integer values for x, or indeed algebraic integers or even p-integral algebraic numbers, the most compelling being the possibility of producing other congruences by differentiation or integration, two workhorses of the *generating functions* arsenal.

Equation (2) bears a strong resemblance to the well-known power series identity

$$\sum_{k=0}^{\infty} \binom{2k}{k} x^k = \frac{1}{\sqrt{1-4x}}, \tag{3}$$

which exhibits the *generating function* for the *central binomial coefficients* $\binom{2k}{k} = (-4)^k \binom{-1/2}{k}$. We contend that the most insightful way to prove congruences such as Equation (2) is to derive them from corresponding power series identities, in this case Equation (3). In this paper we show that this indeed possible in a variety of cases where such similarities occur.

This quite general procedure, which we may call *truncation and reduction modulo p,* may be achieved in simple cases by little more than an appropriate application of the congruence $(1+x)^q \equiv 1 + x^q \pmod{p}$. Incidentally, this also justifies why the range $0 \leq k < q$ generally appears to be a natural summation range to consider for the truncated sums. Equation (2) and its analogue for Catalan numbers will be obtained in this way in Section 2. In Section 3 we will show that *shifted* versions of Equations (1) given in [11], such as

$$\sum_{k=0}^{q-1} \binom{2k}{k+d} \equiv \left(\frac{q-d}{3}\right) \pmod{p} \tag{4}$$

in case of the former, for any $0 \leq d < q$, are also specializations of polynomial congruences, which can be similarly obtained from corresponding power series identities by truncation and reduction modulo p.

We devote the rest of the paper to more sophisticated polynomial congruences which can be obtained by our general method. We focus on a class of series and sums, involving binomial coefficients and generalized harmonic numbers, whose closed forms require polylogarithms and their finite analogues. We describe here only the simplest illustrative example of our results which comes from the known generating function

$$\sum_{k=1}^{\infty} \binom{2k}{k} \frac{x^k}{k} = -2\log\left(\frac{1+\sqrt{1-4x}}{2}\right) = 2\mathrm{Li}_1(\beta),$$

where $\beta = (1-\sqrt{1-4x})/2$ and $\mathrm{Li}_d(x) = \sum_{k=1}^{\infty} x^k/k^d$ denote polylogarithms. An application of our method of truncation and reduction modulo p, where p is an odd prime, produces the congruence

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{x^k}{k} \equiv \pounds_1(\beta) + \pounds_1(1-\beta) \pmod{p},$$

where $\pounds_d(x) = \sum_{k=1}^{p-1} x^k/k^d$ denotes a *finite polylogarithm,* see Section 6 for further details. This congruence is Equation (32) in Theorem 9. Note that the two polylogarithms at the right-hand side of this congruence should be viewed as power series in x, but because of cancellation their sum modulo p turns out to be a polynomial in x. One may also view β as the principal indeterminate with $x = \beta(1-\beta)$ defined in terms of it. We will adopt this point of view, so all our congruences will be between polynomials rather than power series, and our proofs will run much smoother.

A similar truncation procedure can be applied to certain series of the form $\sum_{k=1}^{\infty} \binom{2k}{k} x^k/k^d$ with higher d, but those naturally fit in a wider class of series which admit closed forms involving polylogarithms. Roughly speaking, the series we consider here are generating series of sequences of the general form $\binom{2k}{k} a_k$ or $C_k a_k$, where a_k might be $1/k^d$, or a *generalized harmonic number* $H_k^{(d)} = \sum_{j=1}^{k} 1/j^d$ or possibly a linear combination of products of them. Such series can be conveniently sorted by their *level,* which is the name we give to the highest power of k occurring in the denominator of the expression a_k once expanded. Thus, the series considered so far in this introduction have level zero or one. In Section 5 we exhibit evaluations in closed form for several series of level up to three, quoting several from the literature and producing some new ones. The closed forms of series of level d involve polylogarithms Li_d (and possibly of lower level). As an illustrative example we mention

$$\sum_{k=1}^{\infty} C_k H_k^{(2)} x^{k+1} = 2\beta\,\mathrm{Li}_2(\beta) - (1-\beta)\mathrm{Li}_1(\beta)^2,$$

which is our Equation (21) and gives a closed form for a series of level two.

In Section 7 we apply truncation and reduction modulo p to all series of level up to three considered in Section 5. In the example mentioned above the identity for that series of level two leads to the polynomial congruence

$$\sum_{k=1}^{p-1} C_k H_k^{(2)} x^{k+1} \equiv 2\beta\pounds_2(\beta) + 2(1-\beta)\pounds_2(1-\beta) \pmod{p},$$

for $p > 3$, which is our Equation (38). The right-hand side of this congruence, as well as that of the congruence introduced earlier, and all other congruences we produce in Section 7, exhibits a symmetry with respect to interchanging β and $1-\beta$. This symmetry, which is a necessity as the left-hand side is invariant with respect to this substitution, has no counterpart for the generating functions of the corresponding power series, where this substitution would not even make sense.

The algebraic manipulations of Section 7 will require various functional equations (in the form of congruences) for finite polylogarithms, which we collect in Section 6 after recalling definitions and main properties. This material is well known, and mostly traces back to Mirimanoff in some form [9, p. 61]. However, we provide two new proofs of a 4-term identity (congruence) for the finite logarithm $\pounds_1$ due to Kontsevich [6], which deduce it from the fundamental functional equation for the ordinary logarithmic function by the same methods which inform the present paper.

Another preparatory section is Section 4, where we discuss a certain involutory transform for sequences, given in Equation (10), which we need in the sequel. The transform itself is originally due to Euler, see [10, Equation (1.20)], but the known proof only works in an analytic context where the series involved are assumed to have a positive convergence radius, as it depends on an integral formula for the Hadamard product of power series. We provide a purely algebraic proof, which thus works over any field of characteristic zero. Then we deduce a corresponding truncated version modulo a prime. This congruence is not new either, but our deducing it from its infinite analogue is in line with the spirit of this paper.

In Section 8 we show how our polynomial congruences of Section 7 can be evaluated on special values for x so as to obtain numerical congruences. The main obstacle here is the need for evaluations modulo p in a closed form of the finite polylogarithms involved. Such evaluations, some of which were obtained in [8, Section 4], are available only for a limited set of values of the argument, and fewer so as the level increases. Nevertheless, a number of such congruences can be obtained, and we provide a sample of some new ones.

2. A basic example: central binomial coefficients

The central binomial coefficients have a generating function which we recalled in Equation (3). We will see that the polynomial obtained by omitting all terms of degree at least q from the generating function admits an equally nice closed form when viewed modulo p. The following crucial step is essentially the same which leads to a proof of Lucas' theorem on binomial coefficients modulo p.

Lemma 1. *If q is a power of an odd prime p we have*

$$\sum_{k=0}^{\infty} \binom{2k}{k} x^k \equiv (1-4x)^{(q-1)/2} \cdot \sum_{k=0}^{\infty} \binom{2k}{k} x^{kq} \pmod{p}$$

in the formal power series ring $\mathbb{Z}[[x]]$.

Proof. Recall from Equation (3) that $\sum_{k=0}^{\infty} \binom{2k}{k} x^k = (1-4x)^{-1/2}$. Basic facts about binomial coefficients and Fermat's Little Theorem imply that $(1-4x)^q \equiv 1-(4x)^q \equiv 1-4x^q \pmod{p}$. Therefore, noting that all binomial power series involved have integral coefficients, we have

$$\begin{aligned}(1-4x)^{-1/2} &= (1-4x)^{(q-1)/2}\big((1-4x)^q\big)^{-1/2} \\ &\equiv (1-4x)^{(q-1)/2}(1-4x^q)^{-1/2} \pmod{p},\end{aligned}$$

and the desired conclusion follows. □

By looking at the terms of degree less than q in the congruence of power series given in Lemma 1 we deduce the following polynomial congruence. Its special case $q = p$ appeared in [1, p. 467], where the authors, however, suggested a proof by direct calculation.

Theorem 2. *If q is a power of an odd prime p we have*

$$\sum_{k=0}^{q-1} \binom{2k}{k} x^k \equiv (1-4x)^{(q-1)/2} \pmod{p}.$$

The exclusion of $p = 2$ here is harmless as the central binomial coefficients are all even for $k > 0$. In a formula in $\mathbb{Z}[[x]]$, we have $\sum_{k=0}^{\infty} \binom{2k}{k} x^k \equiv 1 \pmod 2$.

If desired, Lemma 1 readily provides a closed form evaluation modulo p for the sum $\sum_{k=0}^{rq-1} \binom{2k}{k} x^k$, for any given positive integer r, such as

$$\sum_{k=0}^{2q-1} \binom{2k}{k} x^k \equiv (1-4x)^{(q-1)/2}(1+2x^q) \pmod{p}.$$

In the sequel we will disregard such straightforward extensions and focus on the most natural range $0 \le k < q$ for similar sums.

Variations on the congruence of Theorem 2 where the central binomial coefficients are multiplied by fixed powers of k are easily obtained by the familiar device of repeated application of the operator xD, that is, differentiation followed by multiplication by x. As an example, from Theorem 2 we obtain

$$\sum_{k=1}^{q-1} k \binom{2k}{k} x^k \equiv xD(1-4x)^{(q-1)/2} \equiv 2x(1-4x)^{(q-3)/2} \pmod{p} \tag{5}$$

for p odd.

Before we continue we introduce a convenient piece of notation about congruences between power series. By a congruence with respect to a modulus (x^s, p) between power series we mean that the polynomials obtained from them by discarding all terms of degree s or higher have integral coefficients and are congruent modulo p. When both sides have integral coefficients this amounts to equality of their images in the quotient ring $\mathbb{Z}[[x]]/(x^s, p)$. However, it will be convenient to allow ourselves greater flexibility and only require that the coefficients of powers of x of exponents less than s are integers; this does not admit a natural interpretation in terms of quotient rings.

Our next result concerns a polynomial version modulo p of the generating function of the Catalan numbers,

$$\sum_{k=0}^{\infty} C_k x^{k+1} = \frac{1-\sqrt{1-4x}}{2}. \tag{6}$$

This well-known generating function is usually written with both sides divided by x, but the above formulation is more convenient for our present goals. Equation (6) can be obtained by integrating Equation (3) and adjusting the constant term.

Theorem 3. *If q is a power of an odd prime p we have*

$$\sum_{k=0}^{q-1} C_k x^{k+1} \equiv \frac{1-(1-4x)^{(q+1)/2}}{2} - x^q \pmod{p}.$$

As was the case for Theorem 2, the excluded case $p = 2$ in Theorem 2 can easily be dealt with directly, as $\sum_{k=0}^{\infty} C_k x^k \equiv \sum_{i=0}^{\infty} x^{2^i-1} \pmod 2$. From now on we will disregard the case $p = 2$ in our congruences as trivial and easily dealt with separately.

Proof. From Lemma 1 we obtain

$$(1-4x)^{-1/2} \equiv (1-4x)^{(q-1)/2} + 2x^q \pmod{(x^{q+1}, p)},$$

whence

$$(1-4x)^{1/2} = (1-4x)^{-1/2}(1-4x) \equiv (1-4x)^{(q+1)/2} + 2x^q \pmod{(x^{q+1}, p)}.$$

Therefore, we have

$$\sum_{k=0}^{\infty} C_k x^{k+1} = \frac{1-\sqrt{1-4x}}{2} \equiv \frac{1-(1-4x)^{(q+1)/2}}{2} - x^q \pmod{(x^{q+1}, p)},$$

which yields the desired conclusion. □

The congruences of Equation (1), for odd p, follow by evaluation at $x = 1$ of the polynomials of Theorems 2 and 3, using the fact that $(-3)^{(q-1)/2} \equiv \left(\frac{q}{3}\right) \pmod p$. This is easily shown either by using Jacobi symbols and Gauss' quadratic reciprocity law, or by viewing -3 as the discriminant of the polynomial $(x^3 - 1)/(x-1) = x^2 + x + 1$, and then evaluating on -3 the quadratic character of the finite field $\mathbb{F}_q$.

Generating functions of combinatorial sequences which have a similar form as that of the central binomial coefficients admit a similar treatment. We give only one example. The *central trinomial coefficient* T_k is the coefficient of x^k in $(1+x+x^2)^k$. It is well known and easy to prove that these numbers admit the generating function

$$\sum_{k=0}^{\infty} T_k x^k = \big((1-3x)(1+x)\big)^{-1/2} = (1-2x-3x^2)^{-1/2}.$$

Exactly as in the proof of Theorem 2 we find the following congruence.

Theorem 4. *If q is a power of an odd prime p we have*

$$\sum_{k=0}^{q-1} T_k x^k \equiv (1-2x-3x^2)^{(q-1)/2} \pmod p.$$

For example, this shows that for any odd prime we have $\sum_{k=0}^{p-1} T_k \equiv (-1)^{(p-1)/2} \pmod p$, and $\sum_{k=0}^{p-1} (-1)^k T_k \equiv 0 \pmod p$.

3. A variation: shifted central binomial coefficients

In this section we consider *shifted* variants $\binom{2k}{k+d}$ of the central binomial coefficients, as done in [11] and in various papers which followed. We prefer to use $\binom{2k+e}{k}$ instead, which takes care of sums of binomial coefficients $\binom{2k-1}{k+d}$ as well as of $\binom{2k}{k+d}$ at the same time, because the generating function for the corresponding series appears to be better known. For any nonnegative integer e we have

$$\sum_{k\geq 0}\binom{2k+e}{k}x^k = \frac{1}{\sqrt{1-4x}}\left(\frac{1-\sqrt{1-4x}}{2x}\right)^e, \tag{7}$$

see [14, Equation (2.47)]. We will now devise a truncated version modulo p of this equation, over the range $0 \leq k < q$.

Because $\binom{2k+e+q}{k} \equiv \binom{2k+e}{k}$ for $0 \leq k < q$ and $e \geq 0$, according to Lucas' theorem, we may and will assume $0 \leq e < q$. Again because of Lucas' theorem we have $\binom{2k+e}{k} \equiv 0 \pmod p$ for $(q-e)/2 \leq k < q-e$, and also for $q-e/2 \leq k < q$. Hence within the range $0 \leq k < q$, the binomial coefficient can only be nonzero modulo p on the two subintervals $0 \leq k < (q-e)/2$ and $q-e \leq k < q-e/2$. It is convenient to separate the contributions of those two ranges in our polynomial congruence.

Theorem 5. *Let q be a power of an odd prime p, and let $0 \leq e < q$. In the polynomial ring $\mathbb{Z}[\beta]$, setting $x = \beta(1-\beta)$ and $\alpha = 1-\beta$, we have*

$$\sum_{0\leq k<(q-e)/2}\binom{2k+e}{k}x^k \equiv \frac{\alpha^{q-e}-\beta^{q-e}}{\alpha-\beta} \pmod p,$$

and

$$\sum_{0\leq k<q}\binom{2k+e}{k}x^k \equiv \frac{\alpha^{2q-e}-\beta^{2q-e}}{\alpha-\beta} \pmod p.$$

At face value, because of the presence of a denominator the right-hand sides of the congruences in Theorem 5 appear to belong only to the power series ring $\mathbb{Z}[[x]]$, but they are actually polynomials after cancellation takes place. Both congruences extend Theorem 2, which is the special case $e = 0$.

The rationale for introducing a new indeterminate β will be clearer in Section 5, see Equation (13). It is essentially a device to have polynomial congruences in β rather than involving power series in x. In terms of x, the indeterminate β can be taken as the generating function of the Catalan numbers in the form given in Equation (6), that is, $\beta = (1-\sqrt{1-4x})/2$, an element of the power series ring $\mathbb{Z}[[x]]$.

Proof. In terms of β, Equation (7) reads

$$\sum_{k=0}^{\infty}\binom{2k+e}{k}x^k = \frac{1}{(1-2\beta)(1-\beta)^e},$$

which takes place in the power series ring $\mathbb{Q}[[\beta]]$, with $x = \beta(1-\beta)$. However, because all coefficients are integers it actually takes place in $\mathbb{Z}[[x]]$. After multiplying

both sides by $(1-\beta)^e$ and then by $(1-2\beta)^q \equiv 1 \pmod{(\beta^q, p)}$ we obtain

$$(1-\beta)^e \sum_{0\le k<q} \binom{2k+e}{k} x^k \equiv (1-2\beta)^{q-1} \pmod{(\beta^q, p)}. \tag{8}$$

Because the binomial coefficients involved in the left-hand side vanish modulo p for $q - e/2 \le k < q$ the left-hand side is a polynomial of degree less than $2q$ when viewed modulo p, and so the congruence requires the double modulus (β^q, p) to be valid. However, once we restrict the summation range in Equation (8) to those two subintervals where the binomial coefficients may possibly not vanish modulo p, for the higher subinterval we have

$$(1-\beta)^e \sum_{q-e\le k<q-e/2} \binom{2k+e}{k} x^k \equiv \beta^{q-e} \sum_{q-e\le k<q-e/2} \binom{2k+e}{k} x^{k-q+e} \pmod{(\beta^q, p)},$$

because $(1-\beta)^e x^{q-e} = (1-\beta)^q \beta^{q-e} \equiv \beta^{q-e} \pmod{(\beta^q, p)}$. Making this replacement Equation (8) turns it into

$$(1-\beta)^e \sum_{0\le k<(q-e)/2} \binom{2k+e}{k} x^k + \beta^{q-e} \sum_{q-e\le k<q-e/2} \binom{2k+e}{k} x^{k-q+e} \equiv (1-2\beta)^{q-1} \pmod{(\beta^q, p)}.$$

However, the left-hand side of this congruence is now a polynomial of degree less than q (in the indeterminate β). Because so is the right-hand side, the congruence actually holds modulo p.

Now consider the above congruence and the one obtained from it by interchanging the roles of β and $\alpha = 1-\beta$. Taking suitable linear combinations of them we obtain the first congruence of the theorem, as well as

$$\sum_{q-e\le k<q-e/2} \binom{2k+e}{k} x^{k-q+e} \equiv \frac{\alpha^e - \beta^e}{\alpha - \beta} \pmod{p}.$$

Multiplying both sides of this congruence by $x^{q-e} = \alpha^{q-e}\beta^{q-e}$ and adding it to the first congruence of the theorem we obtain the second congruence of the theorem. □

Note the similarity of the congruences of Theorem 5 with Equation (7). However, the congruences are (necessarily) invariant under interchanging β with $\alpha = 1-\beta$, and this fact has no counterpart in Equation (7).

Setting $e = 2d$ in Theorem 5, appropriately shifting the summation range, and considering the vanishing modulo p of the binomial coefficients involved over part of the range, we obtain

$$\sum_{0\le k<q} \binom{2k}{k-d} x^{k-d} \equiv \frac{\alpha^{2q-2d} - \beta^{2q-2d}}{\alpha - \beta} \pmod{p}$$

for $0 \le d < q$. More precisely, this alternate formulation follows directly as described for $0 \le d < q/2$, and after a simple manipulation for $q/2 < d < q$. By

specializing β to be a complex primitive sixth root of unity, whence $x = 1$, we obtain Equation (4) of the Introduction. Variations such as

$$\sum_{0\le k<q} k\binom{2k}{k-d}x^{k-d} \equiv \frac{2\big(\alpha^{2q-2d}-\beta^{2q-2d}\big)x}{(\alpha-\beta)^3} + \frac{d\big(\alpha^{2q-2d}+\beta^{2q-2d}\big)}{(\alpha-\beta)^2} \pmod p$$

can be obtained by a suitable application of the differential operator $\mathrm{d}/\mathrm{d}x = \big(1/(1-2\beta)\big)\cdot \mathrm{d}/\mathrm{d}\beta$.

4. A sequence transform and its modular version

In this section we consider an involutory transform for sequences, which will be needed later in the paper, and show that a truncated version modulo p can be deduced through a similar method as employed in the previous section.

We start by recalling the more well-known *binomial transform*. Given a sequence $(a_n)_{n=0}^{\infty}$ of elements of a field F (or of any ring, for that matter), its *binomial transform* is the sequence (b_n) defined by $b_n = \sum_{k=0}^{n}(-1)^k\binom{n}{k}a_k$, which is more conveniently written as $b_n = \sum_{k=0}^{\infty}(-1)^k\binom{n}{k}a_k$. With our choice of signs (not shared by all authors) the binomial transform is *involutory,* meaning that it coincides with the inverse transform, and hence $a_n = \sum_{k=0}^{\infty}(-1)^k\binom{n}{k}b_k$. An easy way to see this is noting that the exponential generating functions $\tilde{A}(x) = \sum_{k=0}^{\infty} a_k x^k/k!$ and $\tilde{B}(x) = \sum_{k=0}^{\infty} b_k x^k/k!$ are related by $\tilde{B}(x) = \exp(-x)\cdot\tilde{A}(-x)$.

Here we are interested in the related transform

$$\sum_{k=0}^{\infty}\binom{2k}{k}a_k x^k = \frac{1}{\sqrt{1-4x}}\sum_{k=0}^{\infty}\binom{2k}{k}b_k\left(\frac{-x}{1-4x}\right)^k, \tag{9}$$

where (a_n) and (b_n) are connected by the binomial transform. Writing $\binom{2k}{k} = (-4)^k\binom{-1/2}{k}$, Equation (9) follows from the following more general fact by evaluating at $y = -1/2$.

Proposition 6. *Let F be a field of characteristic zero. In the ring $\big(F[y]\big)[[x]]$ we have*

$$\sum_{k=0}^{\infty}\binom{y}{k}a_k x^k = (1+x)^y\sum_{k=0}^{\infty}\binom{y}{k}b_k\left(\frac{x}{1+x}\right)^k, \tag{10}$$

where $a_k \in F$ and $b_n = \sum_{k=0}^{\infty}(-1)^k\binom{n}{k}a_k$ for all $n \ge 0$.

By definition we have $(1+x)^y = \sum_{k=0}^{\infty}\binom{y}{k}x^k$, which belongs to $\big(\mathbb{Q}[y]\big)[[x]] \subseteq \big(F[y]\big)[[x]]$. The expected property $(1+x)^{y_1+y_2} = (1+x)^{y_1}\cdot(1+x)^{y_2}$ holds, and takes place in $\big(\mathbb{Q}[y_1,y_2]\big)[[x]]$. For sequences of complex numbers, and with complex parameter in place of the indeterminate y (and with a different sign choice) Proposition 6 is [2, Proposition 5], but in essence the result traces back to Euler, see [10, Equation (1.20)].

To be precise, the special version of Proposition 6 proved in [2] also requires that $\sum_{k=0}^{\infty} a_k x^k$ has a positive radius of convergence. This is because that proof amounts to viewing the left-hand side of Equation (10) as the Hadamard (that is,

termwise) product of the series $\sum_{k=0}^{\infty}\binom{y}{k}x^k$ and $\sum_{k=0}^{\infty}a_kx^k$ and applying a familiar integral formula for it (see [3, Chapter 1, Exercise 30]). Our purely algebraic approach below bypasses the analytic tool and allows us to attain the greater generality of Proposition 6. For example, one can obtain *parametrized* versions by taking F to be a function field.

Proof of Proposition 6. Fix an index $N \geq 0$. If we change all a_k with $k > N$ into zeroes, then $b_k = \sum_{j=0}^{\infty}(-1)^j\binom{k}{j}a_j$ change accordingly, but b_k remains unchanged for $k \leq N$. The coefficient of x^N in either side of Equation (10) is unaffected by this change. Thus, in proving Equation (10) we may assume that $a_k = 0$ for $k > N$. This artifice will save us the trouble of working with bilateral Laurent series, which of course do not form a ring.

Introduce a further indeterminate z, so that we have

$$b_k = \sum_{j=0}^{k}(-1)^j\binom{k}{j}a_j = [z^0]\left((-1)^k(1-z)^k\sum_{j=0}^{N}a_jz^{-j}\right)$$

in the ring $R((z))$ of formal Laurent series over the integral domain $R = \big(F[y]\big)[[x]]$. Hence

$$\begin{aligned}
\sum_{k=0}^{\infty}\binom{y}{k}b_k\left(\frac{-x}{1+x}\right)^k &= \sum_{k=0}^{\infty}\binom{y}{k}\left(\frac{-x}{1+x}\right)^k\cdot[z^0]\left((1-z)^k\sum_{j=0}^{N}a_jz^{-j}\right)\\
&= [z^0]\left(\sum_{k=0}^{\infty}\binom{y}{k}\left(\frac{x(z-1)}{(1+x)}\right)^k\sum_{j=0}^{N}a_jz^{-j}\right)\\
&= [z^0]\left(\left(1+\frac{x(z-1)}{(1+x)}\right)^y\sum_{j=0}^{N}a_jz^{-j}\right)\\
&= (1+x)^{-y}\cdot[z^0]\left((1+xz)^y\sum_{j=0}^{N}a_jz^{-j}\right)\\
&= (1+x)^{-y}\cdot\sum_{k=0}^{N}\binom{y}{k}a_kx^k.
\end{aligned}$$

The conclusion follows upon multiplication by $(1+x)^y$. □

Now we show how similar arguments as in Section 2 allow one to deduce from Equation (9) a truncated version modulo a prime. For simplicity of exposition we work with sequences of rational numbers, but it will be clear that it extends to more general contexts if needed, such as number fields. Thus, let q be a power of an odd prime p, let $a_0, a_1, \ldots, a_{q-1}$ be p-integral rational numbers, and set $b_n = \sum_{k=0}^{n}(-1)^k\binom{n}{k}a_k$ for $0 \leq n < q-1$. Then in $\mathbb{Q}[x]$ we have the congruence

$$\sum_{k=0}^{q-1}\binom{2k}{k}a_kx^k \equiv (1-4x)^{(q-1)/2}\sum_{k=0}^{q-1}\binom{2k}{k}b_k\left(\frac{-x}{1-4x}\right)^k \pmod{p}. \tag{11}$$

Equation (11) is not hard to establish directly, as in [13, Section 3], but deriving it from Equation (9) is more in line with the spirit of this paper. To do that, extend the finite sequence (a_k) to an infinite sequence by setting $a_k = 0$ for $k \geq q$, and let (b_k) be the binomial transform of (a_k). Hence Equation (9) holds and, consequently,

$$\sum_{k=0}^{q-1} \binom{2k}{k} a_k x^k \equiv \frac{1}{\sqrt{1-4x}} \sum_{k=0}^{q-1} \binom{2k}{k} b_k \left(\frac{-x}{1-4x}\right)^k \pmod{(x^q, p)}.$$

Using $(1-4x)^{-1/2} \equiv (1-4x)^{(q-1)/2}(1-4x^q)^{-1/2} \pmod{p}$ as in the proof of Lemma 1 we obtain that Equation (11) holds modulo (x^q, p). However, because $\binom{2k}{k} \equiv 0 \pmod{p}$ for $q < 2k < 2q$ we may restrict the summation range in the right-hand side of Equation (11) to $0 \leq (q-1)/2$, thus making both sides polynomials of degree less than p, whence Equation (11) holds modulo p, as desired.

5. Some generating series evaluated in terms of polylogarithms

In this section we recall a few known generating series involving polylogarithms, and introduce some new ones, towards the goal of truncating them and obtaining polynomial congruences modulo a prime in Section 7. All our series will be generating series of sequences of the general form $\binom{2k}{k} a_k$ or $C_k a_k$, where a_k might be $1/k^d$, or a generalized harmonic number $H_k^{(d)} = \sum_{j=1}^{k} 1/j^d$ (where the ordinary harmonic numbers are $H_k = H_k^{(1)}$), or possibly a linear combination of products of them. For the sake of classification we will informally call *the level* of such a generating series the highest power of k which occurs in the denominator of a_k once expanded. Some such generating series can be evaluated in closed form in terms of polylogarithmic series

$$\mathrm{Li}_d(x) = \sum_{k=1}^{\infty} \frac{x^k}{k^d} \tag{12}$$

with d equal to the level of the series, and the ordinary logarithmic series. However, we will systematically write $\mathrm{Li}_1(x)$ in place of the equivalent notation $-\log(1-x)$ in our formulas. This will be more natural in view of deducing congruences modulo a prime in Section 7.

We may and will work in a formal setting, viewing all series involved as formal power series, say in $\mathbb{Q}[[x]]$ or $\mathbb{C}[[x]]$, as subsequent evaluations inside the disk of convergence pose no challenge when desired. Thus, polylogarithms $\mathrm{Li}_d(x)$ will be simply defined by Equation (12) for any integer d, and no issue of analytic continuation will arise. Note that $\mathrm{Li}_0(x) = x/(1-x)$. Differentiation and integration will be done on a formal level in $\mathbb{Q}[[x]]$. In particular, note that

$$x \cdot \frac{\mathrm{d}}{\mathrm{d}x} \mathrm{Li}_d(x) = \mathrm{Li}_{d-1}(x).$$

Because (a slight variant of) the generating function of the Catalan numbers will occur repeatedly we conveniently assign a name to it, namely,

$$\beta := \sum_{k=0}^{\infty} C_k x^{k+1} = \frac{1-\sqrt{1-4x}}{2}. \tag{13}$$

It satifies $\beta(1-\beta) = x$. The generating series of the central binomial coefficients can also be expressed in terms of β, namely, $\sum_{k=0}^{\infty} \binom{2k}{k} x^k = 1/(1-2\beta) = \mathrm{d}\beta/\mathrm{d}x$. According to our terminology these two series are the generating series of level zero. Series with general term $C_k a_k$ can be obtained by integration from the corresponding ones with term $\binom{2k}{k} a_k$, and so our initial focus will be on the latter. Integration of the corresponding closed forms will present no obstacle in the cases of our concern. Our notation for indefinite integration will assume that the arbitrary constant involved will be suitably adjusted, allowing us to write $\int (1-2\beta)^{-1} \mathrm{d}x = \beta$, for example.

From each series of level d one can obtain another series of the same level by an application of the involutory transform described by Equation (9). Going from a series of level d to a series of level $d+1$ may be achieved by integration. Thus, the easiest generating series of level one is obtained by integrating the generating series of the central binomial coefficients divided by x. As pointed out in [7, Equation (6)], this yields

$$\sum_{k=1}^{\infty} \binom{2k}{k} \frac{x^k}{k} = -2\log(1-\beta) = 2\mathrm{Li}_1(\beta). \tag{14}$$

An application of the transform of Equation (9) turns this into another series of level one, obtained by Boyadzhiev in [2, Theorem 1]. In our notation in terms of β, that result concisely reads

$$\sum_{k=1}^{\infty} \binom{2k}{k} H_k x^k = \frac{-2}{1-2\beta} \mathrm{Li}_1\left(\frac{\beta}{2\beta-1}\right) = 2\frac{\mathrm{Li}_1(2\beta) - \mathrm{Li}_1(\beta)}{1-2\beta}. \tag{15}$$

These are just two of several equivalent expressions for this series, due to the functional equation $\log(1+x+y+xy) = \log(1+x)\log(1+y)$. The former expression may appear more convenient due to the single occurrence of Li_1, but the latter will soon prove to be more compatible with analogues of higher level, and more amenable to reduction modulo a prime in the next section.

Our collection of series of level one is completed with two corresponding series involving the Catalan numbers. The analogue of Equation (14), which reads

$$\sum_{k=1}^{\infty} C_k \frac{x^{k+1}}{k} = \sum_{k=1}^{\infty} \binom{2k}{k} \frac{x^{k+1}}{k} - \sum_{k=1}^{\infty} C_k x^{k+1} = 2x\mathrm{Li}_1(\beta) - \beta + x, \tag{16}$$

is obtained from Equations (14) and (13) noting that $1/\big(k(k+1)\big) = 1/k - 1/(k+1)$. Alternatively, Equation (16) can be found by integrating Equation (14). Finally,

integrating Equation (15) in either form we obtain

$$\sum_{k=1}^{\infty} C_k H_k x^{k+1} = \mathrm{Li}_1(\beta) + (1-2\beta)\mathrm{Li}_1\left(\frac{\beta}{2\beta-1}\right) \tag{17}$$
$$= -(1-2\beta)\mathrm{Li}_1(2\beta) + 2(1-\beta)\mathrm{Li}_1(\beta),$$

which is equivalent to [2, Corollary 2]. We should mention that Equation (17) can also be obtained from Equation (16) through an application of the transform expressed by Equation (9).

Boyadzhiev also produced closed forms for some generating series of level two in [2, Equations (24) and (25)]. Those expressions involve several values of Li_1 and Li_2, and also irrational constants such as $\log 2$ and π. However, with some sacrifice on their range of validity (which is irrelevant in the present context) and by means of standard functional equations for polylogarithms, they amount to the simpler formulations

$$\sum_{k=1}^{\infty} \binom{2k}{k} \frac{x^k}{k^2} = 2\mathrm{Li}_2(\beta) - \mathrm{Li}_1(\beta)^2, \tag{18}$$

and

$$\sum_{k=1}^{\infty} \binom{2k}{k} \frac{H_k}{k} x^k = -2\mathrm{Li}_2\left(\frac{\beta}{2\beta-1}\right) - \mathrm{Li}_1\left(\frac{\beta}{2\beta-1}\right)^2. \tag{19}$$

They are obtained by integrating Equations (14) and (15) after division by x. Companion generating series of Equations (18) and (19) with the Catalan numbers may be readily obtained using $1/\big(k(k+1)\big) = 1/k - 1/(k+1)$.

In the next result we contribute two further generating series of level two, which involve the generalized harmonic numbers $H_k^{(2)}$.

Theorem 7. *We have*

$$\sum_{k=1}^{\infty} \binom{2k}{k} H_k^{(2)} x^k = \frac{2\mathrm{Li}_2(\beta) + \mathrm{Li}_1(\beta)^2}{1-2\beta}, \tag{20}$$

and

$$\sum_{k=1}^{\infty} C_k H_k^{(2)} x^{k+1} = 2\beta\,\mathrm{Li}_2(\beta) - (1-\beta)\mathrm{Li}_1(\beta)^2. \tag{21}$$

Proof. Note that

$$\sum_{j=1}^{k} \binom{k}{j} (-1)^j H_j^{(2)} = -\frac{H_k}{k},$$

according to an easy summation by parts. Now Equation (20) can be obtained from Equation (19) through the transform of Equation (9), as follows:

$$\begin{aligned}\sum_{k=1}^{\infty}\binom{2k}{k}H_k^{(2)}x^k &= \frac{1}{1-2\beta}\sum_{k=1}^{\infty}\binom{2k}{k}\left(\frac{-x}{1-4x}\right)^k\sum_{j=1}^{k}\binom{k}{j}(-1)^j H_j^{(2)}\\ &= -\frac{1}{1-2\beta}\sum_{k=1}^{\infty}\binom{2k}{k}\frac{H_k}{k}\left(\frac{-x}{1-4x}\right)^k\\ &= \frac{2\mathrm{Li}_2(\beta)+\mathrm{Li}_1(\beta)^2}{1-2\beta}.\end{aligned}$$

Equation (21) can be obtained from Equation (20) through integration. In fact, integration by parts yields

$$\int\frac{\mathrm{Li}_2(\beta)}{1-2\beta}\,\mathrm{d}x = \int\mathrm{Li}_2(\beta)\mathrm{d}\beta = \beta\mathrm{Li}_2(\beta)+(1-\beta)\mathrm{Li}_1(\beta)-\beta$$

and

$$\int\frac{\mathrm{Li}_1(\beta)^2}{1-2\beta}\,\mathrm{d}x = \int\mathrm{Li}_1(\beta)^2\,\mathrm{d}\beta = (\beta-1)\mathrm{Li}_1(\beta)^2+2(\beta-1)\mathrm{Li}_1(\beta)+2\beta,$$

whence Equation (21) follows. □

Finally, we evaluate one generating series of level three in closed form, where two suitable summands are combined.

Theorem 8. *We have*

$$\sum_{k=1}^{\infty}\binom{2k}{k}\left(\frac{H_k^{(2)}}{k}+\frac{1}{k^3}\right)x^k = 4\,\mathrm{Li}_3(\beta)+\frac{2}{3}\mathrm{Li}_1(\beta)^3. \tag{22}$$

Proof. We start with noting that for $d\geq 1$ we have

$$\frac{\mathrm{d}}{\mathrm{d}x}\mathrm{Li}_d(\beta) = \frac{\mathrm{Li}_{d-1}(\beta)}{\beta(1-2\beta)},\quad\text{and}\quad\frac{\mathrm{d}}{\mathrm{d}x}\mathrm{Li}_1(\beta)^d = \frac{d\mathrm{Li}_1(\beta)^{d-1}}{(1-\beta)(1-2\beta)}.$$

Adding up the left-hand sides of Equations (20) and (18), dividing by x and integrating, yields

$$\begin{aligned}\sum_{k=1}^{\infty}\binom{2k}{k}\left(\frac{H_k^{(2)}}{k}+\frac{1}{k^3}\right)x^k &= \int\left(\frac{2\mathrm{Li}_2(\beta)+\mathrm{Li}_1(\beta)^2}{x(1-2\beta)}+\frac{2\mathrm{Li}_2(\beta)-\mathrm{Li}_1(\beta)^2}{x}\right)\mathrm{d}x\\ &= 4\int\frac{\mathrm{Li}_2(\beta)}{\beta(1-2\beta)}\,\mathrm{d}x+2\int\frac{\mathrm{Li}_1(\beta)^2}{(1-\beta)(1-2\beta)}\,\mathrm{d}x\\ &= 4\,\mathrm{Li}_3(\beta)+\frac{2}{3}\mathrm{Li}_1(\beta)^3,\end{aligned}$$

as claimed. □

6. Congruences for finite polylogarithms

In Section 7 we will obtain congruences for finite sums modulo a prime p from the generating series found in Section 5. Because each of those involves some polylogarithm Li_d, we give here a brief introduction to their finite analogues $\pounds_d$. For a fixed prime p, the *finite polylogarithms* can be defined by truncating the polylogarithmic series just before the term of degree p, namely,

$$\pounds_d(x) = \sum_{k=1}^{p-1} \frac{x^k}{k^d}. \tag{23}$$

Although they will be mostly viewed modulo p, hence over the field $\mathbb{F}_p$, there is an advantage in having them defined as polynomials with rational coefficients. Thus, we have $\pounds_d(x) \equiv \mathrm{Li}_d(x) \pmod{x^p}$ in the power series ring $\mathbb{Q}[[x]]$ and, in particular, $\pounds_1(x) \equiv -\log(1-x) \pmod{x^p}$. Note also that $\pounds_0(x) = (x-x^p)/(1-x)$.

When $p=2$ we have $\pounds_d(x) = x$ for all d, which is not very interesting. Nor is the behaviour of the central binomial coefficients $\binom{2k}{k}$ or the Catalan numbers C_k when viewed modulo 2, as we already pointed out right after stating Theorems 2 and 3. Thus, we set the blanket assumption $p > 2$ in what follows and leave to the interested reader the task of checking what remains true or fails in that case. More generally, because $\pounds_{d+p-1}(x) \equiv \pounds_d(x) \pmod{p}$, an assumption $0 < d < p$ would not be too demanding in most places, but we need not require that from the outset.

We will need the congruence

$$\pounds_1(x)^d \equiv (-1)^{d-1} d! \cdot \pounds_d(1-x) \pmod{(x^p, p)}, \tag{24}$$

valid for $0 < d < p-1$, which is a weaker version of a more precise congruence, modulo (x^{p+1}, p), tracing back to Mirimanoff and involving a Bernoulli number. A proof of that, with a further discussion, can be found in [8, Lemma 3.2].

For small values of d, Equation (24) can be refined to a congruence modulo p, namely,

$$\pounds_1(x) \equiv \pounds_1(1-x) \pmod{p}, \tag{25}$$

$$\pounds_1(x)^2/2 \equiv -x^p \pounds_2(x) - (1-x^p)\pounds_2(1-x) \pmod{p}, \tag{26}$$

$$\begin{aligned}\pounds_1(x)^3/6 \equiv\ & x^p \pounds_3(x) + (1-x^p)\pounds_3(1-x) + x^{2p}(1-x^p)\pounds_3(1-1/x) \\ & + (2/3)x^p(1-x^p)\pounds_3(-1) \pmod{p};\end{aligned} \tag{27}$$

the second congruence clearly requires $p > 2$, and the third one $p > 3$. As explained in [8, Section 3], these congruences have been recently rediscovered by several authors, but they were already known to Mirimanoff [9, p. 61]. Equation (25) is a plain consequence of

$$\pounds_1(x) \equiv \frac{-x^p - (1-x)^p + 1}{p} \pmod{p}, \tag{28}$$

which is easily proved by expanding $(1-x)^p$ and using the fact that $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1} \equiv (-1)^{k-1} p \pmod{p^2}$ for $0 < k < p$. The invariance of $\pounds_1(x)$ under the substitution

$x \mapsto 1-x$, due to Equation (25), combines with invariance under another involutory transformation, expressed by the obvious congruence $\mathcal{L}_1(x) \equiv -x^p \mathcal{L}_1(1/x) \pmod{p}$, to give invariance under a certain (celebrated) group G of transformations, isomorphic with the symmetric group on three letters. In [8, Section 3] we showed how this symmetry group allows one to lift a proof of Equations (26) and (27) from the fact that they hold modulo (x^{p+1}, p) according to Mirimanoff's slightly more precise version of Equation (24) given in [8, Lemma 3.2].

By suitably composing the two involutory transformations of $\mathcal{L}_1(x)$ given above we find

$$\mathcal{L}_1(x) \equiv \mathcal{L}_1(1-x) \equiv (x-1)^p \mathcal{L}_1\left(\frac{1}{1-x}\right) \equiv (x-1)^p \mathcal{L}_1\left(\frac{x}{x-1}\right) \pmod{p},$$

which corresponds to invariance under the third involution in the mentioned symmetry group G. The congruence between the first and last expressions may be viewed as a version for $\mathcal{L}_1(x)$ of the property

$$-\log(1-x) = \log\left(1 - \frac{x}{x-1}\right) \tag{29}$$

of the logarithmic series; in fact, viewing both sides of the latter modulo (x^p, p) yields the former modulo (x^p, p). It turns out that the fundamental two-variable functional equation for the logarithmic series, which we may write in the form

$$-\log(1-x) + \log(1-y) = \log\left(\frac{1-y}{1-x}\right) \tag{30}$$

and has Equation (29) as its special case for $y = 0$, also has analogue for $\mathcal{L}_1(x)$, namely,

$$\mathcal{L}_1(x) - \mathcal{L}_1(y) + x^p \mathcal{L}_1\left(\frac{y}{x}\right) + (1-x)^p \mathcal{L}_1\left(\frac{1-y}{1-x}\right) \equiv 0 \pmod{p}. \tag{31}$$

Because of the polynomials appearing as denominators this may be viewed in the ring of power series $\mathbb{Z}_p[[x, y]]$, where $\mathbb{Z}_p$ denotes the ring of p-adic integers, but it actually takes place in the polynomial ring $\mathbb{Z}_p[x, y]$ after cancellation. It seems to have been first noticed by Kontsevich [6] in a more rudimentary form, where $\mathcal{L}_1$ is viewed as a map from $\mathbb{F}_p$ to itself, in order to point out an analogy of $\mathcal{L}_1$ with the *binary entropy function* of information theory. Kontsevich sketched a proof of his version of Equation (31), which amounts to Equation (31) viewed modulo the ideal $(x^p - x, y^p - y, p)$ of $\mathbb{Z}_p[x, y]$, by direct calculation after expanding the various $\mathcal{L}_1$ involved. That argument can certainly be upgraded to a full proof of Equation (31), which, however, would not be too illuminating. Elbaz-Vincent and Gangl, in a much more general scheme (greatly motivated by [6]) where functional equations for $\mathcal{L}_d$ are deduced from functional equations for Li_{d+1}, gave another proof of Equation (31) in [4, Proposition 5.9]. While that proof is certainly clarifying, understanding it requires mastering a large part of their paper.

We now give two elementary and self-contained new proofs of Equation (31). The former is slightly longer but more in line with the spirit of this paper, as it emphasizes and exploits the connection with Equation (30), the functional equation for the ordinary logarithm.

First proof of Equation (31). Viewing Equation (30) modulo the ideal $(x,y)^p$ of $\mathbb{Q}[[x,y]]$, rewriting in terms of $\pounds_1$, and then reducing modulo p, we find

$$\pounds_1(x) - \pounds_1(y) + \pounds_1\left(1 - \frac{1-y}{1-x}\right) \equiv 0 \pmod{((x,y)^p, p)}$$

in $\mathbb{Z}_p[[x,y]]$. Rewriting the last summand using $\pounds_1(1-z) \equiv \pounds_1(z) \pmod p$ we conclude that Equation (31) holds modulo $((x,y)^p, p)$. Because the left-hand side of Equation (31) is a polynomial of degree not exceeding p, the residual indeterminacy about terms of degree exactly p could be abundantly resolved using the invariance of $\pounds_1$ under the group G of transformations, by argument similar to those in [8]. However, a simple alternative is checking that the terms of degree p in Equation (31) cancel out modulo p. In fact, the homogeneous part of degree p in the polynomial

$$(1-x)^p \pounds_1\left(\frac{1-y}{1-x}\right) = \sum_{k=1}^{p-1} \frac{(1-x)^{p-k}(1-y)^k}{k}$$

equals $(-1)^p \sum_{k=1}^{p-1} x^{p-k}y^k/k \equiv -x^p \pounds_1(y/x) \pmod p$. □

Second proof of Equation (31). Applying Equation (28) to each of the four summands of Equation (31) yields, in particular,

$$x^p \pounds_1\left(\frac{y}{x}\right) \equiv \frac{-y^p - (x-y)^p + x^p}{p} \pmod p,$$

which is a sort of homogeneous version of Equation (28), and

$$(1-x)^p \pounds_1\left(\frac{1-y}{1-x}\right) \equiv \frac{-(1-y)^p - (y-x)^p + (1-x)^p}{p} \pmod p.$$

Because $(-1)^p \equiv -1 \pmod p$ and $(1-x)^p \equiv 1 - x^p \pmod p$, all summands in Equation (31) cancel out, as desired. □

7. Obtaining polynomial congruences by truncation

After these preliminaries on finite polylogarithms we proceed with producing analogues with finite sums modulo p from the generating series considered in Section 5. We start by deducing three congruences involving central binomial coefficients, of level one, two, and three, from the corresponding generating series, which are Equations (14), (18), and (22). We collect them together because of the similarity of their right-hand sides. Because of integers coprime with p appearing as denominators we conveniently state those congruences, and all congruences to follow, in the polynomial ring $\mathbb{Z}_p[\beta]$, where $\mathbb{Z}_p$ is the ring of p-adic integers and $x = \beta(1-\beta)$.

Theorem 9. *Let $p > 3$ be a prime. The following congruences hold in the polynomial ring $\mathbb{Z}_p[\beta]$, where $x = \beta(1-\beta)$ and $\alpha = 1-\beta$:*

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{x^k}{k} \equiv \pounds_1(\alpha) + \pounds_1(\beta) \pmod{p}, \tag{32}$$

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{x^k}{k^2} \equiv 2\pounds_2(\alpha) + 2\pounds_2(\beta) \pmod{p}, \tag{33}$$

$$\sum_{k=1}^{p-1} \binom{2k}{k} \left(\frac{H_k^{(2)}}{k} + \frac{1}{k^3} \right) x^k \equiv 4\pounds_3(\alpha) + 4\pounds_3(\beta) \pmod{p}. \tag{34}$$

Proof. To prove Equation (32) we start with writing Equation (14) in the equivalent form

$$\sum_{k=1}^{\infty} \binom{2k}{k} \frac{\big(\beta(1-\beta)\big)^k}{k} = 2\mathrm{Li}_1(\beta),$$

in the power series ring $\mathbb{Q}[[\beta]]$. Because $\mathrm{Li}_d(x) \equiv \pounds_d(x) \pmod{x^p}$ we have

$$\sum_{k=1}^{(p-1)/2} \binom{2k}{k} \frac{\big(\beta(1-\beta)\big)^k}{k} \equiv 2\pounds_1(\beta) \pmod{\beta^p}$$

in $\mathbb{Q}[[\beta]]$. Now both sides are polynomials with p-integral rational coefficients, and hence can be viewed modulo p. Thus, the same congruence holds modulo the ideal (β^p, p) of $\mathbb{Z}_p[\beta]$. Because both sides are polynomials of degree less than p, the congruence actually holds modulo p (that is, modulo the ideal (p) of $\mathbb{Z}_p[\beta]$). This is equivalent to the more symmetric Equation (32) because $\pounds_1(1-\beta) \equiv \pounds_1(\beta) \pmod{p}$ according to Equation (25).

To prove Equation (33) we proceed similarly, writing Equation (18) in the equivalent form

$$\sum_{k=1}^{\infty} \binom{2k}{k} \frac{\big(\beta(1-\beta)\big)^k}{k^2} = 2\mathrm{Li}_2(\beta) - \mathrm{Li}_1(\beta)^2,$$

in $\mathbb{Q}[[\beta]]$. Truncating the series and using Equation (24) we deduce the congruence

$$\sum_{k=1}^{(p-1)/2} \binom{2k}{k} \frac{\big(\beta(1-\beta)\big)^k}{k^2} \equiv 2\pounds_2(\beta) + 2\pounds_2(1-\beta) \pmod{(\beta^p, p)}$$

in $\mathbb{Z}_p[\beta]$. Now both sides are polynomials of degree less than p, and hence the congruence actually holds modulo p as well, which is the desired conclusion.

In an entirely similar manner one obtains Equation (34) from Equation (22), again using Equation (24) to get rid of $\pounds_1(\beta)^3$ in favour of $\pounds_3(\alpha)$. □

According to need, the congruences of Theorem 9 can be viewed as identities in the polynomial ring $\mathbb{F}_p[\beta]$ or in the power series ring $\mathbb{F}_p[[x]]$, with β the power series defined by Equation (13). Taking the former viewpoint, the left-hand sides belong to the subfield $\mathbb{F}_p(x)$ of the field $\mathbb{F}_p(\beta)$ of rational expressions fixed by the

automorphism which interchanges β and $\alpha = 1 - \beta$. This invariance is emphasized by the form in which we have written the right-hand sides. Viewing the congruences as between polynomials in β, rather than power series in x, has the advantage of allowing evaluation on algebraic integers, as we will exemplify in Section 8.

Next we present two further congruences of level one, which are finite analogues of Equations (15) and (17) found by Boyadzhev.

Theorem 10. *Let p be an odd prime. The following congruences hold in the polynomial ring $\mathbb{Z}_p[\beta]$, where $x = \beta(1-\beta)$ and $\alpha = 1 - \beta$:*

$$\sum_{k=1}^{p-1} \binom{2k}{k} H_k x^k \equiv -2(\alpha-\beta)^{p-1} \pounds_1\left(\frac{\beta}{\beta-\alpha}\right) \pmod{p}, \tag{35}$$

$$\sum_{k=1}^{p-1} C_k H_k x^{k+1} \equiv \pounds_1(\beta) + (\alpha-\beta)^{p+1} \pounds_1\left(\frac{\beta}{\beta-\alpha}\right) \pmod{p}. \tag{36}$$

The right-hand sides of Equations (35) and (36) are actually polynomials, once $\pounds_1$ is expanded into a sum and cancellation with the power of $\alpha - \beta$ takes place. Also, invariance under interchanging α and β holds because $\pounds_1\big(\alpha/(\alpha-\beta)\big) \equiv \pounds_1\big(\beta/(\beta-\alpha)\big) \pmod{p}$ and $\pounds_1(\alpha) = \pounds_1(\beta)$, according to Equation (25).

Note that Equations (35) and (36) relate to their infinite counterparts, Equations (15) and (17), much in the same way as the congruences given in Theorems 2 and 3 relate to their infinite counterparts, the generating functions of the central binomial coefficients and the Catalan numbers.

Proof. One may obtain Equation (35) from Equation (16) by means of the transform given in Equation (11), in the same way as in Section 5 we deduced Equation (15) from Equation (14) using the transform of Equation (9). However, keeping with the spirit of this paper we rather deduce the congruence from the corresponding identity of power series, Equation (15).

After rewriting Equation (15) in the equivalent form

$$(1-2\beta)\sum_{k=1}^{\infty} \binom{2k}{k} H_k\big(\beta(1-\beta)\big)^k = 2\mathrm{Li}_1(2\beta) - 2\mathrm{Li}_1(\beta)$$

in the power series ring $\mathbb{Q}[[\beta]]$, we infer the congruence

$$(1-2\beta)\sum_{k=1}^{(p-1)/2} \binom{2k}{k} H_k\big(\beta(1-\beta)\big)^k \equiv 2\pounds_1(2\beta) - 2\pounds_1(\beta) \pmod{\beta^p},$$

which now takes place in the polynomial ring $\mathbb{Q}[\beta]$. The right-hand side is a polynomial of degree less than p, while the left-hand side is a polynomial of degree not exceeding p. Its term of degree p is

$$-2\beta\binom{p-1}{(p-1)/2} H_{(p-1)/2}(-\beta^2)^{(p-1)/2} \equiv -2H_{(p-1)/2}\beta^p \equiv -2\pounds_1(-1)\beta^p \pmod{p},$$

because

$$H_{(p-1)/2} = 2\sum_{k=1}^{p-1} \frac{1}{2k} = \pounds_1(1) + \pounds_1(-1) \equiv \pounds_1(-1) \pmod{p}.$$

Consequently, reduction modulo p yields the polynomial congruence

$$(1-2\beta) \sum_{k=1}^{(p-1)/2} \binom{2k}{k} H_k\big(\beta(1-\beta)\big)^k \equiv 2\pounds_1(2\beta) - 2\pounds_1(\beta) - 2\pounds_1(-1)\beta^p \pmod{p}.$$

To turn this congruence into the more symmetric form stated in the theorem, note that $\pounds(-1) = \pounds_1(2) = -2\pounds_1(1/2)$, apply Equations (31) and (25) to transform half the right-hand side into

$$\begin{aligned}\pounds_1(2\beta) - \pounds_1(\beta) + 2\beta^p\pounds_1(1/2) &\equiv -(1-2\beta)^p \pounds_1\left(\frac{1-\beta}{1-2\beta}\right) \pmod{p} \\ &\equiv (2\beta-1)^p \pounds_1\left(\frac{\beta}{2\beta-1}\right) \pmod{p},\end{aligned}$$

and finally divide both sides of the resulting congruence by $1-2\beta$.

Like Equation (35), Equation (36) may be obtained in several ways, one of which is deducing it from the generating function for the corresponding series, Equation (17). For a change, we will obtain Equation (36) from Equation (35) through integration, noting that

$$\frac{\mathrm{d}}{\mathrm{d}\beta} \sum_{k=1}^{p-1} C_k H_k x^{k+1} = (1-2\beta) \sum_{k=1}^{p-1} \binom{2k}{k} H_k x^k.$$

Because of the identities

$$x \cdot \frac{\mathrm{d}}{\mathrm{d}\beta}\pounds_1(x) = \pounds_0(x) = \frac{x - x^p}{1-x}$$

we have

$$(2\beta-1)^p \pounds_0\left(\frac{\beta}{2\beta-1}\right) = \frac{\beta(2\beta-1)^p - \beta^p(2\beta-1)}{(\beta-1)} \equiv \frac{\beta-\beta^p}{(1-\beta)} = \pounds_0(\beta) \pmod{p}$$

and, consequently,

$$(1-2\beta)^{p+1} \cdot \frac{\mathrm{d}}{\mathrm{d}\beta}\pounds_1\left(\frac{\beta}{2\beta-1}\right) = \frac{(1-2\beta)^p}{\beta} \cdot \pounds_0\left(\frac{\beta}{2\beta-1}\right) \equiv -\pounds_0(\beta) \pmod{p}.$$

It follows that

$$\begin{aligned}&\frac{\mathrm{d}}{\mathrm{d}\beta}\left(\pounds_1(\beta) + (1-2\beta)^{p+1}\pounds_1\left(\frac{\beta}{2\beta-1}\right)\right) \\ &\quad\equiv \frac{\pounds_0(\beta)}{\beta} + (1-2\beta)^p \cdot \frac{\mathrm{d}}{\mathrm{d}\beta}\left((1-2\beta)\pounds_1\left(\frac{\beta}{2\beta-1}\right)\right) \pmod{p} \\ &\quad\equiv -2(1-2\beta)^p \pounds_1\left(\frac{\beta}{2\beta-1}\right) \pmod{p}.\end{aligned}$$

This proves that the difference of the two sides of Equation (36), which is clearly a polynomial in $\mathbb{Z}_p[\beta]$ with no constant term and of degree not exceeding $p+1$, has zero derivative modulo p. Hence that difference can be taken to be an integral multiple of $p\beta^p$. However, because both sides of the congruence vanish for $\beta = 1$, that difference must be the zero polynomial modulo p. □

Moving on to congruences of level two, we have already produced the simplest one, which is Equation (33). We conclude this section with establishing three further congruences of level two. The first two are analogues of Equations (20) and (21).

Theorem 11. *Let $p > 3$ be a prime. The following congruences hold in the polynomial ring $\mathbb{Z}_p[\beta]$, where $x = \beta(1-\beta)$ and $\alpha = 1-\beta$:*

$$\sum_{k=1}^{p-1} \binom{2k}{k} H_k^{(2)} x^k \equiv \frac{2\pounds_2(\alpha) - 2\pounds_2(\beta)}{\beta - \alpha} \pmod{p}, \tag{37}$$

$$\sum_{k=1}^{p-1} C_k H_k^{(2)} x^{k+1} \equiv 2\alpha\pounds_2(\alpha) + 2\beta\pounds_2(\beta) \pmod{p}. \tag{38}$$

Proof. We will deduce the congruence in Equation (37) from the corresponding identity in Equation (20). Thus, we start with rewriting that in the equivalent form

$$(1-2\beta)\sum_{k=1}^{\infty} \binom{2k}{k} H_k^{(2)} \big(\beta(1-\beta)\big)^k = 2\mathrm{Li}_2(\beta) + \mathrm{Li}_1(\beta)^2$$

in the power series ring $\mathbb{Q}[[\beta]]$. Truncating the series and using Equation (24) we deduce the congruence

$$(1-2\beta)\sum_{k=1}^{(p-1)/2} \binom{2k}{k} H_k^{(2)} \big(\beta(1-\beta)\big)^k = 2\pounds_2(\beta) - 2\pounds_2(1-\beta) \pmod{(\beta^p, p)}$$

in $\mathbb{Z}_p[\beta]$. Now both sides are polynomials of degree less than p, and hence the congruence actually holds modulo p as well. Equation (37) follows after dividing by $1-2\beta$ and recalling that $\binom{2k}{k}$ vanishes modulo p for $p/2 < k < p$.

In a similar fashion, we will deduce Equation (38) from Equation (21). After rewriting the latter as

$$\sum_{k=1}^{\infty} C_k H_k^{(2)} \big(\beta(1-\beta)\big)^{k+1} = 2\beta\mathrm{Li}_2(\beta) - (1-\beta)\mathrm{Li}_1(\beta)^2$$

in the formal power series ring $\mathbb{Q}[[\beta]]$, because $\mathrm{Li}_d(\beta)/\beta \equiv \pounds_d(\beta)/\beta \pmod{\beta^{p-1}}$ we deduce the congruence

$$\sum_{k=1}^{(p-1)/2} C_k H_k^{(2)} \big(\beta(1-\beta)\big)^{k+1} \equiv 2\beta\pounds_2(\beta) - (1-\beta)\pounds_1(\beta)^2 \pmod{\beta^{p+1}}.$$

Because both sides are polynomials with p-integral rational coefficients, they can be viewed modulo p. Now Equation (24) only yields $\pounds_1(\beta)^2 \equiv 2\pounds_2(1-\beta)$

$(\mathrm{mod}\ (\beta^p, p))$. However, this congruence actually holds modulo (β^{p+1}, p), because of the more precise Equation (26) together with the fact that $\mathcal{L}_2(1) \equiv 0 \pmod{p}$. (Alternatively, use the sharper version of Equation (24) given in [8, Lemma 3.2] and the fact that the Bernoulli number B_{p-2} vanishes, again for $p > 3$.) Thus, our congruence takes the form

$$\sum_{k=1}^{(p-1)/2} C_k H_k^{(2)} \big(\beta(1-\beta)\big)^{k+1} \equiv 2\beta \mathcal{L}_2(\beta) + 2(1-\beta)\mathcal{L}_2(1-\beta) \pmod{(\beta^{p+1}, p)}$$

in $\mathbb{Z}_p[\beta]$. Because both sides are polynomials of degree not exceeding p, this congruence actually holds modulo p, rather than just modulo (β^{p+1}, p). Finally, because $C_k \equiv 0 \pmod{p}$ for $p/2 < k < p-1$, and $H_{p-1}(2) \equiv 0 \pmod{p}$, we can extend the summation range to $0 < k < p$, and our congruence takes the desired final form. □

Another congruence of level two is an analogue of Equation (19), namely,

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{H_k}{k} x^k \equiv 2(\alpha-\beta)^p \left(\mathcal{L}_2\left(\frac{\alpha}{\alpha-\beta}\right) - \mathcal{L}_2\left(\frac{\beta}{\beta-\alpha}\right)\right) \pmod{p}, \tag{39}$$

also to be read in the polynomial ring $\mathbb{Z}_p[\beta]$, where $x = \beta(1-\beta)$ and $\alpha = 1-\beta$, for $p > 2$. Note that invariance of the right-hand side under interchanging α and β is manifest in this case. It may be possible to deduce Equation (39) from Equation (19) by truncation using similar arguments to those used so far, but it seems simpler to obtain it from Equation (37) by means of the sequence transform of Equation (11). In fact, this procedure is followed in [13], where Equation (39) appears as [13, Equation (13)]. The same paper contains a similar derivation of our Equation (35), which appears there as [13, Equation (12)].

8. Some applications to numerical congruences

In this last section we present some examples of interesting numerical congruences which can be obtained by evaluating some of our polynomial congruences to particular values of x. We limit ourselves to a selection of the most elegant ones.

In Equation (22) we have found a closed form for the sum of the two series $\sum_{k=1}^{\infty} \binom{2k}{k} H_k^{(2)} x^k/k$ and $\sum_{k=1}^{\infty} \binom{2k}{k} x^k/k^3$, but it may not be possible to do so for the individual series. However, closed forms modulo p can be found for the two analogous finite sums, thus refining Equation (34). In fact, an evaluation modulo p of the former was essentially found in [8], namely,

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{H_k^{(2)}}{k} x^k \equiv -2x^p(\mathcal{L}_3(1-1/\alpha) + \mathcal{L}_3(1-1/\beta)) \pmod{p}, \tag{40}$$

for $p > 3$. To see this, according to [8, Equation (38)] we have

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{H_k^{(2)}}{k} x^k \equiv -2x^p \sum_{k=1}^{p-1} \frac{v_k(2-1/x)}{k^3} \pmod{p},$$

where $\sum_{k=1}^{p-1} v_k(y)/k^d = \pounds_d(\gamma) + \pounds_d(\gamma^{-1})$ with $\gamma^2 - y\gamma + 1 = 0$, as described in [8, Section 5] with slight notational changes. Because the roots of the quadratic equation $\gamma^2-(2-1/x)\gamma+1 = 0$ are precisely our $1-1/\alpha$ and $1-1/\beta$, Equation (40) follows. Now, subtracting Equation (40) from Equation (34) we find

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{x^k}{k^3} \equiv 4\pounds_3(\alpha)+4\pounds_3(\beta)+2x^p(\pounds_3(1-1/\alpha)+\pounds_3(1-1/\beta)) \pmod{p}. \tag{41}$$

Equation (41) is noteworthy because it had appeared unaccessible to the methods of [8], where we only obtained versions with lower powers of k at the denominator in place of k^3, see [8, Theorem 7.1]. Thus, we can now supplement the sample numerical congruences given in [8, Section 8] with some obtained through specializations of the polynomial congruence of Equation (41), such as

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{1}{k^3} \equiv \frac{2B_{p-3}}{3} \pmod{p}, \tag{42}$$

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{(-2)^k}{k^3} \equiv -\frac{8q_p(2)^3 + 31B_{p-3}}{12} \pmod{p}, \tag{43}$$

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{1}{4^k k^3} \equiv \frac{4q_p(2)^3 + 2B_{p-3}}{3} \pmod{p}, \tag{44}$$

$$\sum_{k=1}^{p-1} \frac{(-1)^k}{k^3} \binom{2k}{k} (L_{3k} - 1) \equiv -\frac{3}{5}\left(q_L^3 + 2B_{p-3}\right) \pmod{p}; \tag{45}$$

the first three congruences hold for any prime $p > 3$, and the fourth one requires $p > 5$. Here B_n denotes a Bernoulli number, $q_p(2) = (2^{p-1} - 1)/2$ is a Fermat quotient, L_n denotes a Lucas number, and $q_L = (L_p - 1)/p$ is a Lucas quotient. Equation (42) appeared in [5, Theorem 2], but the others appear to be new. For the reader's convenience, the following table lists the required values of α, β, and the related quantities which appear in Equation (41).

x	α	β	$1-1/\alpha$	$1-1/\beta$
1	ω_6	ω_6^{-1}	ω_6	ω_6^{-1}
-2	2	-1	$1/2$	2
$1/4$	$1/2$	$1/2$	-1	-1
-1	ϕ_+	ϕ_-	ϕ_-^2	ϕ_+^2
$-\phi_+^3$	ϕ_+^2	$-\phi_+$	$-\phi_-$	ϕ_+
$-\phi_-^3$	$-\phi_-$	ϕ_-^2	ϕ_-	$-\phi_+$

Here ω_6 is a primitive complex sixth root of unity, and $\phi_\pm = (1 \pm \sqrt{5})/2$. Equations (42), (43), and (44) follow at once by appropriately evaluating Equation (41) and using the congruences produced in [8, Section 4] for the required values of $\pounds_3$.

Equations (45) is slightly more complicated and requires three evaluations of Equation (41), corresponding to the three last rows of the above table. In fact, because $L_n = \phi_+^n + \phi_-^n$ the left-hand side of Equation (45) can be written as

$$\sum_{k=1}^{p-1} \frac{(-\phi_+^3)^k}{k^3}\binom{2k}{k} + \sum_{k=1}^{p-1} \frac{(-\phi_-^3)^k}{k^3}\binom{2k}{k} - \sum_{k=1}^{p-1} \frac{(-1)^k}{k^3}\binom{2k}{k}.$$

According to Equation (41) this is congruent, modulo p, to a certain linear combination of values of $\pounds_3$. The desired conclusion follows from congruences for some of those values given in [8, Theorem 4.4] and an application of standard congruences for polylogarithms recalled in [8, Section 2]. Unfortunately, we are not able to supplement Equations (42)–(45) with a similar evaluation of the sum $\sum_{k=1}^{p-1}\big((-1)^k/k^3\big)\binom{2k}{k}$, for example, because from [8] we know evaluations modulo p of $\pounds_3(\phi_\pm^2)$, but not of $\pounds_3(\phi_\pm)$.

References

[1] Roland Bacher and Robin Chapman. Symmetric Pascal matrices modulo p. *European J. Combin.*, 25(4):459–473, 2004.

[2] Khristo N. Boyadzhiev. Series with central binomial coefficients, Catalan numbers, and harmonic numbers. *J. Integer Seq.*, 15(1):Article 12.1.7, 11, 2012.

[3] Louis Comtet. *Advanced combinatorics*. D. Reidel Publishing Co., Dordrecht, enlarged edition, 1974. The art of finite and infinite expansions.

[4] Philippe Elbaz-Vincent and Herbert Gangl. On poly(ana)logs. I. *Compositio Math.*, 130(2):161–210, 2002.

[5] Khodabakhsh Hessami Pilehrood and Tatiana Hessami Pilehrood. Congruences arising from Apéry-type series for zeta values. *Adv. in Appl. Math.*, 49(3-5):218–238, 2012.

[6] Maxim Kontsevich. The $1\frac{1}{2}$-logarithm. Appendix to: "On poly(ana)logs. I" [Compositio Math **130** (2002), no. 2, 161–210; MR1883818 (2002m:11059)] by P. Elbaz-Vincent and H. Gangl. *Compositio Math.*, 130(2):211–214, 2002.

[7] Derrick H. Lehmer. Interesting series involving the central binomial coefficient. *Amer. Math. Monthly*, 92(7):449–457, 1985.

[8] Sandro Mattarei and Roberto Tauraso. Congruences for central binomial sums and finite polylogarithms. *J. Number Theory*, 133(1):131–157, 2013.

[9] Dmitry Mirimanoff. L'équation indéterminée $x^l + y^l + z^l = 0$ et le critérium de Kummer. *J. Reine Angew. Math.*, 128:45–68, 1905.

[10] Niels E. Nørlund. Hypergeometric functions. *Acta Math.*, 94:289–349, 1955.

[11] Hao Pan and Zhi-Wei Sun. A combinatorial identity with application to Catalan numbers. *Discrete Math.*, 306(16):1921–1940, 2006.

[12] Zhi-Wei Sun. Binomial coefficients, Catalan numbers and Lucas quotients. *Sci. China Math.*, 53(9):2473–2488, 2010.

[13] Roberto Tauraso. Some congruences for central binomial sums involving Fibonacci and Lucas numbers. *J. Integer Seq.*, 19(5):Article 16.5.4, 10, 2016.

[14] Herbert S. Wilf. *generatingfunctionology*. A K Peters, Ltd., Wellesley, MA, third edition, 2006.

E-mail address: smattarei@lincoln.ac.uk

School of Mathematics and Physics, University of Lincoln, Brayford Pool, Lincoln, LN6 7TS, United Kingdom

E-mail address: tauraso@mat.uniroma2.it

Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy