Journal of Number Theory 133 (2013) 131–157

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Congruences for central binomial sums and finite polylogarithms

Sandro Mattarei [a], Roberto Tauraso [b,*]

[a] Dipartimento di Matematica, Università di Trento, via Sommarive 14, 38123 Trento, Italy
[b] Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy

ARTICLE INFO

Article history:
Received 28 October 2011
Revised 27 March 2012
Accepted 1 May 2012
Available online 15 September 2012
Communicated by David Goss

Keywords:
Congruences
Bernoulli numbers
Binomial coefficients
Polylogarithm
Finite sums

ABSTRACT

Text. We prove congruences, modulo a power of a prime p, for certain finite sums involving central binomial coefficients $\binom{2k}{k}$, partly motivated by analogies with the well-known power series for $(\arcsin z)^2$ and $(\arcsin z)^4$. The right-hand sides of those congruences involve values of the finite polylogarithms $\mathcal{L}_d(x) = \sum_{k=1}^{p-1} x^k/k^d$. Exploiting the available functional equations for the latter we compute those values, modulo the required powers of p, in terms of familiar quantities such as Fermat quotients and Bernoulli numbers.

Video. For a video summary of this paper, please click here or visit http://www.youtube.com/watch?v=W54Ad0YFr8A.

1. Introduction

A well-known power series expansion of a familiar function where central binomial coefficients appear in the denominators is

$$2\big(\arcsin(z/2)\big)^2 = \sum_{k=1}^{\infty} \frac{1}{k^2\binom{2k}{k}} z^{2k},$$

which yields $\sum_{k=1}^{\infty} k^{-2}\binom{2k}{k}^{-1} = \pi^2/18 = \zeta(2)/3$ upon setting $z = 1$. By appropriate successive applications of differentiation one can derive explicit closed-form expressions for the power series $\sum_{k=1}^{\infty} k^{-d}\binom{2k}{k}^{-1} t^k$, for any integer $d \leqslant 2$, and corresponding specializations to interesting values

* Corresponding author.
E-mail addresses: mattarei@science.unitn.it (S. Mattarei), tauraso@mat.uniroma2.it (R. Tauraso).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.05.036

of t. For $d > 2$ the sum of that power series appears not to be expressible in terms of the simpler transcendental functions, but explicit evaluations at special values of t are still possible, such as $\sum_{k=1}^{\infty}(-1)^k k^{-3}\binom{2k}{k}^{-1} = -2\zeta(3)/5$ and $\sum_{k=1}^{\infty} k^{-4}\binom{2k}{k}^{-1} = 17\zeta(4)/36$. The former played a role in Apery's celebrated proof of irrationality of $\zeta(3)$, see van der Poorten's account of Apery's proof [28] for a discussion of both formulas and relevant references. Evaluation of the series for d up to 8 when $t = 1$, and d up to 9 when $t = -1$, were found in [2], exploiting special values of polylogarithms whose availability depends on *polylogarithm ladders* [10], and hence, ultimately, on functional equations satisfied by the classical polylogarithms $\mathrm{Li}_d(z) = \sum_{k=1}^{\infty} z^k/k^d$.

In a different direction, the power series expansions for $(\arcsin z)^m$ were determined in [3], extending on the known results for $m = 1, \ldots, 4$ (see [1, pp. 262–263], for example). Besides certain types of *multiple harmonic sums,* the coefficients involve a central binomial coefficient in the numerator for m odd, and in the denominator for m even. Of special interest for us is the case $m = 4$, which reads

$$\frac{2}{3}\big(\arcsin(z/2)\big)^4 = \sum_{k=1}^{\infty} \frac{H_{k-1}(2)}{k^2\binom{2k}{k}} z^{2k}, \tag{1}$$

where $H_{k-1}(2) = \sum_{r=1}^{k-1} 1/r^2$. Again, differentiation produces similar closed-form expressions for the sums of analogous power series with k or 1 in place of the factor k^2 at the denominator (as in [4], for example).

Finite modular versions of familiar power series play a role in various parts of algebra and number theory, where a power series is truncated at an appropriate place leaving a polynomial with p-integral coefficients, which can then be evaluated modulo p. Part of the functional properties of the sum of the infinite series may be preserved in that polynomial. A distinguished algebraic example is the crucial role of the truncated exponential series $\sum_{k=0}^{p-1} x^k/k!$ in the theory of modular Lie algebras, as a tool for *toral switching* [17, Chapter 1]: little is preserved of the functional equation $\exp(x + y) = \exp(y)\exp(y)$, but just enough to make the algebraic application work, see [11] for an extension of this point of view. As an example from number theory we mention the use of the partial sum $\sum_{k=1}^{p-1} x^k/k$ of the logarithmic series $-\log(1 - x)$ made in [8]: there a polynomial argument about the partial sum is strongly motivated by transcendence arguments for the logarithmic function. Generally speaking, when an infinite power series with rational coefficients admits an explicit summation formula it is natural to seek for finite modular analogues, that is, for congruences modulo p or a power of p for an appropriate truncated version of the series, and to see how far those resemble the original function.

In this note we consider the sums of the first $p - 1$ terms of some of the series mentioned earlier, where p is a prime, and evaluate them modulo certain powers of p. Specifically, we obtain congruences for the polynomials

$$p\sum_{k=1}^{p-1} \frac{t^k}{k^d\binom{2k}{k}} \pmod{p^3} \quad \text{and} \quad p\sum_{k=1}^{p-1} \frac{H_{k-1}(2)}{k^d\binom{2k}{k}} t^k \pmod{p}, \tag{2}$$

where p is a prime and $d = 0, 1, 2$ (and possibly $d = 3, 4$ as well, as we discuss at the end of this Introduction), which we then specialize to particular values of t. (Multiplication by p is needed to make the resulting coefficients p-integral.) Special cases of the second type of sum above were considered by Z.W. Sun in [23] together with related sums, for certain values of t, and with attention to a comparison with the corresponding infinite sums. As we explain in our Section 8, our results include a few congruences first obtained in [23]. However, we produce many new ones in a systematic way, and provide a framework to possibly obtain more. As a test of the validity of this approach we prove several conjectures formulated by Z.W. Sun in [21].

A crucial observation is that, in analogy with the corresponding infinite sums, explicit evaluation of the sums in Eq. (2) for specific values of t depends on the availability of special values of the *finite polylogarithms*, defined as

$$\mathcal{L}_d(x) = \sum_{k=1}^{p-1} \frac{x^k}{k^d},$$

where d is a positive integer. In turn, the possibility of computing those modulo small powers of p is due to the existence of several known functional equations (in the form of congruences) satisfied by the finite polylogarithms, which we collect in Section 2.

It is fair to assume that much of this material on finite polylogarithms was known to Mirimanoff at the beginning of the twentieth century. In fact, two special functional equations (modulo p) relating $\mathcal{L}_1(x)^2$ and $\mathcal{L}_1(x)^3$ to values of $\mathcal{L}_2$ and $\mathcal{L}_3$, which were rediscovered in [7] and [5], were explicitly mentioned by Mirimanoff in [13, p. 61]. Because Mirimanoff omitted the proofs, and the proofs by algebraic manipulations given in [7] and [5] tend to hide how such equations might be discovered in the first place, we devote Section 3 to presenting our own proofs of those polynomial congruences. The crux of our argument is that while the initial coefficients of $\mathcal{L}_1(x)^2$ and $\mathcal{L}_1(x)^3$ are easy to obtain as in the characteristic-zero case, invariance under a certain (rather illustrious) symmetry group of order six allows one to recover all of the remaining coefficients.

For certain special values of x the available functional equations for finite polylogarithms taken together provide enough information to determine $\mathcal{L}_d(x)$ modulo p, for $d = 1, 2, 3$. We present these evaluations in Section 4.

In Sections 5 and 6 we establish the necessary connection between the sums in Eq. (2) and values of finite polylogarithms. This does require some work, which we split into two parts and outline here. The first part, in Section 5, is to produce polynomial identities (that is, in characteristic zero) which express our sums in Eq. (2) as more tractable sums involving *Dickson polynomials*. Because Dickson polynomials satisfy second-order linear recurrence relations, certain sums in which they appear can be expressed in terms of finite polylogarithms. However, bringing the sums of Section 5 to the required form requires passing from polynomial identities to suitable polynomial congruences, which we do in Section 6.

We devote Section 7 to simpler-looking polynomials obtained from those in Eq. (2) by switching the central binomial coefficients from the denominators to the numerators. Congruences for them cannot, generally speaking, be inferred from the corresponding ones for the polynomials in Eq. (2), but they can be obtained by similar methods, and also involve values of the finite polylogarithms.

Our final Section 8 brings together the two main streams of this paper, namely, the finite polylogarithms studied in Sections 2, 3 and 4, and the polynomial congruences developed through Sections 5, 6 and 7. The polynomial congruences for the sums in Eq. (2) and their analogues with the central binomial coefficients in the numerators can be evaluated at the special values of t for which we have computed the relevant finite polylogarithmic values in Section 4. Many numerical congruences can be obtained in this way, and we restrain ourselves to display a selection of the most interesting ones, which include several conjectured by Z.W. Sun.

A few words are appropriate to comment on our restriction $d \leqslant 2$ for the polynomials in Eq. (2). In principle, our polynomial identities in Section 5 can be extended to higher values of d, each case following from the previous one by appropriate integration. In fact, the third identity in our Theorem 5.2 is for $d = 3$, and then leads to the congruence in Theorem 6.2. In Section 8 we apply the corresponding polynomial identity with $d = 4$ without actually stating it; one can find it quoted in [15]. However, it does not appear feasible to obtain pleasant numerical congruences from those polynomial identities for higher values of d.

The authors are grateful to the referee for his/her careful reading of the manuscript.

2. General congruences for $\mathcal{L}_d(x)$

In this section we collect some functional equations modulo a prime p and other relations satisfied by the finite polylogarithms, especially $\mathcal{L}_1$, $\mathcal{L}_2$ and $\mathcal{L}_3$, which we will use in the rest of the paper. Some of them are related to functional equations satisfied by the classical polylogarithms (see [9]);

a procedure for deducing them from the latter is described in [6]. The following most basic identities actually hold for all finite polylogarithms $\mathcal{L}_d$:

- the inversion relation [6, Proposition 5.7(1)], and its extension modulo p^2 [20, Lemma 4.3],

$$\mathcal{L}_d(x) \equiv (-1)^d x^p \mathcal{L}_d(1/x) \pmod{p}, \tag{3}$$

$$\mathcal{L}_d(x) \equiv (-1)^d x^p \mathcal{L}_d(1/x) - dp\mathcal{L}_{d+1}(x) \pmod{p^2}; \tag{4}$$

- the distribution relation [6, Proposition 5.7(2)],

$$\mathcal{L}_d\big(x^m\big) \equiv m^{d-1} \sum_{k=0}^{m-1} \left(\sum_{j=0}^{m-1} \big(\omega_m^k x\big)^{pj} \right) \mathcal{L}_d\big(\omega_m^k x\big) \pmod{p}, \quad \text{where } \omega_m = e^{2\pi i/m}; \tag{5}$$

of course this congruence takes place in the ring of integers of the cyclotomic field $\mathbb{Q}(\omega)$.

Next, there are several relations which are specific to $\mathcal{L}_1$, $\mathcal{L}_2$ and $\mathcal{L}_3$. Some of them involve the quantities

$$q_p(x) = \frac{x^{p-1} - 1}{p} \quad \text{and} \quad Q_p(x) = \frac{x^p + (1-x)^p - 1}{p} = xq_p(x) + (1-x)q_p(1-x),$$

and some require $p > 3$, which we assume from now on for simplicity. They are as follows:

- the 3-term relation for $\mathcal{L}_2$ [6, Proposition 5.11], rediscovered in [7, Eq. (5)],

$$\mathcal{L}_2(x) \equiv \mathcal{L}_2(1-x) + x^p \mathcal{L}_2(1-1/x) \pmod{p}; \tag{6}$$

- a congruence noted by Granville [7, Eq. (6)],

$$Q_p(x) \equiv -\mathcal{L}_1(1-x) - p\mathcal{L}_2(x) \pmod{p^2}; \tag{7}$$

- another congruence rediscovered by Granville [7, Eq. (5)], but see [13, p. 61],

$$\frac{1}{2} Q_p^2(x) \equiv -x^p \mathcal{L}_2(x) - \big(1 - x^p\big)\mathcal{L}_2(1-x) \pmod{p}; \tag{8}$$

- a congruence rediscovered by Dilcher and Skula [5, Theorem 2], but see [13, p. 61],

$$\frac{1}{6} Q_p^3(x) \equiv -x^p \mathcal{L}_3(x) - \big(1 - x^p\big)\mathcal{L}_3(1-x) - x^{2p}\big(1 - x^p\big)\mathcal{L}_3(1-1/x) - \frac{2}{3} x^p \big(1 - x^p\big)\mathcal{L}_3(-1) \pmod{p}. \tag{9}$$

We will also need a special case of the following congruence, obtained by the authors in [12, Lemma 3.2]: for $p > d+1$

$$\sum_{0<k_1<k_2<\cdots<k_d<p} \frac{x^{k_d}}{k_1 k_2 \cdots k_d} \equiv (-1)^{d-1} \mathcal{L}_d(1-x) \pmod{p}. \tag{10}$$

We mention for completeness that the easy congruence (4) can be extended as follows modulo arbitrary powers of p,

$$(-1)^d x^p \mathcal{L}_d(1/x) = \sum_{m=0}^{\infty} \binom{d+m-1}{m} p^m \mathcal{L}_{d+m}(x), \tag{11}$$

to be interpreted in the power series ring $\mathbb{Z}_p[[x]]$.

Proof of Eq. (11). We have

$$\begin{aligned}(-1)^d x^p \mathcal{L}_d(1/x) &= (-1)^d \sum_{k=1}^{p-1} \frac{x^{p-k}}{k^d} = (-1)^d \sum_{k=1}^{p-1} \frac{x^k}{(p-k)^d} \\ &= \sum_{k=1}^{p-1} \frac{x^k}{k^d} \left(1 - \frac{p}{k}\right)^{-d} \\ &= \sum_{k=1}^{p-1} \frac{x^k}{k^d} \sum_{m=0}^{\infty} \binom{d+m-1}{d} (p/k)^m \\ &= \sum_{m=0}^{\infty} \binom{d+m-1}{m} p^m \mathcal{L}_{d+m}(x),\end{aligned}$$

as desired. □

3. New proofs of congruences (6), (8) and (9)

The proofs of Eqs. (6), (7) and (8) given in [7], and that of Eq. (9) in [5], were obtained by algebraic manipulations after differentiation of both sides. An undesirable feature of such proofs is that one is required to guess the desired congruence in the first place. We present proofs of Eqs. (6), (8) and (9) which do not suffer from this imperfection.

Because of the congruence

$$Q_p(x) \equiv -\mathcal{L}_1(x) \pmod{p}, \tag{12}$$

which plainly follows from the definition of $Q(x)$ by expanding $(1-x)^p$ and using the fact that $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1} \equiv (-1)^{k-1} p/k \pmod{p^2}$ for $0 < k < p$, Eqs. (8) and (9) are seen to be equivalent to the second and third of the following set of three congruences:

$$\mathcal{L}_1(x) \equiv \mathcal{L}_1(1-x) \pmod{p}, \tag{13}$$

$$\mathcal{L}_1(x)^2/2 \equiv -x^p \mathcal{L}_2(x) - \left(1-x^p\right)\mathcal{L}_2(1-x) \pmod{p}, \tag{14}$$

$$\begin{aligned}\mathcal{L}_1(x)^3/6 \equiv{}& x^p \mathcal{L}_3(x) + \left(1-x^p\right)\mathcal{L}_3(1-x) + x^{2p}\left(1-x^p\right)\mathcal{L}_3(1-1/x) \\ &+ (2/3)x^p\left(1-x^p\right)\mathcal{L}_3(-1) \pmod{p};\end{aligned} \tag{15}$$

the second congruence clearly requires $p > 2$, and the third one $p > 3$. The first of these three congruences follows from Eq. (12) and the obvious invariance of $Q_p(x)$ under the substitution $x \mapsto 1-x$. The remaining two were already known to Mirimanoff [13, p. 61], as we pointed out in the Introduction. Note that the terms of degree less than p in the right-hand sides of the three congruences are

given by $\mathcal{L}_1(1-x)$, $-\mathcal{L}_2(1-x)$ and $\mathcal{L}_3(1-x)$. It is easy to see that these terms match the corresponding terms in the left-hand sides. In fact, this statement appropriately extends to powers $\mathcal{L}_1(x)^d$ for arbitrary d, as we show in Lemma 3.2 below, including some extra terms as well. It follows that congruences (14) and (15) are verified up to and including the term of degree p. Then we will recover all the remaining terms in the right-hand sides of Eqs. (14) and (15), and thus complete their proofs, by invariance under a group of transformations of order six, generated by the symmetry expressed by Eq. (13) together with the other obvious symmetry $\mathcal{L}_1(x) \equiv -x^p \mathcal{L}_1(1/x) \pmod p$, which is a special case of Eq. (3). In case of Eq. (14), where only about half the coefficients need to be recovered, the argument yields a proof of Eq. (6) as a by-product. The group of transformations of order six has a long history, being omnipresent in the investigations on Fermat's last theorem, see [16], and it is a fair guess that Mirimanoff's own proofs of congruences (14) and (15) might have had much in common with ours.

Because $\mathcal{L}_1(x) \equiv -\log(1-x) \pmod{x^p}$, we start the ball rolling by studying the coefficients in the powers of the ordinary logarithmic series.

Lemma 3.1. *For any nonnegative integers d, k, the coefficient of x^k in the power series*

$$\log^d(1+x)/d! \in \mathbb{Q}[[x]]$$

equals the coefficient of y^d in the polynomial

$$\binom{y}{k} = y(y-1)\cdots(y-k+1)/k! \in \mathbb{Q}[y].$$

Proof. The identity

$$\exp\bigl(y\log(1+x)\bigr) = (1+x)^y$$

yields

$$\sum_{d=0}^{\infty} \bigl(y\log(1+x)\bigr)^d/d! = \sum_{k=0}^{\infty} \binom{y}{k} x^k,$$

with both series converging for (x, y) in a suitable neighborhood of the origin in $\mathbb{R}^2$ (or $\mathbb{C}^2$). Hence the latter identity holds in the ring of formal power series $\mathbb{Q}[[x, y]]$, and the conclusion follows. □

Our usage of polynomial congruences with respect to a double modulus (x^m, p) will be to give precedence to the modulus x^m over the modulus p, in the sense that we interpret them as congruences modulo p after all terms of degree m or higher have been discarded (regardless of their coefficients).

Lemma 3.2. *For $1 < d < p-1$ we have*

$$\mathcal{L}_1(x)^d/d! \equiv (-1)^{d-1}\mathcal{L}_d(1-x) + (-1)^d \frac{B_{p-d}}{d} x^p \pmod{\bigl(x^{p+1}, p\bigr)},$$

where B_{p-d} denotes a Bernoulli number.

Proof. The terms of degree less than p in the polynomial $\mathcal{L}_1(x)$ coincide with the corresponding terms of the power series $-\log(1-x)$. Because there is no constant term, Lemma 3.1 implies that the

coefficient of x^k in the polynomial $\mathcal{L}_1(x)^d/d!$, for $k < p+d-1$, equals $(-1)^{d+k}$ times the coefficient of y^d in the polynomial $\binom{y}{k} \in \mathbb{Q}[y]$. In particular, this holds for $k \leqslant p$, which is all we need here.

As for the first term at the right-hand side of the congruence, we have

$$\mathcal{L}_d(1-x) = \sum_{r=1}^{p-1} \frac{(1-x)^r}{r^d} = \sum_{r=1}^{p-1} \frac{1}{r^d} \sum_{k=0}^{p-1} \binom{r}{k} (-x)^k = \sum_{k=0}^{p-1} \left(\sum_{r=1}^{p-1} \frac{1}{r^d} \binom{r}{k} \right) (-x)^k.$$

Because $\sum_{r=1}^{p-1} r^h \equiv -1 \pmod p$ if $p-1 \mid h$, and $\equiv 0 \pmod p$ otherwise, after expanding $\binom{r}{k}$ as a polynomial in r we see that the sum

$$\sum_{r=1}^{p-1} \frac{1}{r^d} \binom{r}{k} = \sum_{r=1}^{p-1} \frac{1}{r^d} \left(a_k r^k + \cdots + a_1 r + a_0 \right)$$

is congruent, modulo p, to the opposite of the coefficient of y^d in the polynomial $\binom{y}{k} \in \mathbb{Q}[y]$, for $k < p$. This proves that the stated congruence holds modulo (x^p, p).

We deal with the coefficient of x^p noting that

$$\binom{y}{p} = \frac{y}{p} \prod_{j=1}^{p-1} \left(1 - \frac{y}{j} \right) = \frac{y}{p} \sum_{r=0}^{p-1} h_r (-y)^r,$$

where

$$h_r = \sum_{0 < j_1 < j_2 < \cdots < j_r < p} \frac{1}{j_1 j_2 \cdots j_r}.$$

According to [31], for $1 \leqslant r \leqslant p-3$ we have

$$h_r \equiv \frac{(-1)^{r-1}}{r+1} p B_{p-r-1} \pmod{p^2},$$

which completes the proof. □

The congruence in Lemma 3.2 traces back to Mirimanoff. With little extra effort the above proof extends it to a congruence modulo (x^{p+d-1}, p) involving Stirling numbers of the first kind besides Bernoulli numbers.

According to Lemma 3.2 the term of degree p in $\mathcal{L}_d(x)^d$ vanishes modulo p when d is even. An alternative route to this conclusion is noting that the polynomial $\binom{y}{p} - (y^p - y)/p$ has p-integral coefficients and that its reduction modulo p is an odd polynomial in $\mathbb{F}_p[y]$, which is easy to check by evaluating it on $y = 0, 1, \ldots, p-1$.

Lemma 3.2 tells us that congruence (14) is correct as far as we look only at the terms of degree up to p. To complete the proof we now use the available symmetries.

Proof of Eqs. (6) and (14). According to Eq. (3) we have $\mathcal{L}_1(x)^2 \equiv x^{2p} \mathcal{L}_1(1/x)^2 \pmod p$. This means that the coefficients of x^k and x^{2p-k} in $\mathcal{L}_1(x)^2$ are equivalent modulo p, for all k. But the values modulo p of the lower half of the coefficients are given in Lemma 3.2, namely, $\mathcal{L}_1(x)^2/2 \equiv -\mathcal{L}_2(1-x) \pmod{(x^{p+1}, p)}$. Hence this determines the upper half of the coefficients as well, and so we have

$$\mathcal{L}_1(x)^2/2 \equiv -\mathcal{L}_2(1-x) - x^{2p} \mathcal{L}_2(1-1/x) \pmod p. \tag{16}$$

Because the left-hand side is invariant, modulo p, under the substitution $x \mapsto 1-x$, so must be the right-hand side, and hence

$$-\mathcal{L}_2(1-x) - x^{2p}\mathcal{L}_2(1-1/x) \equiv -\mathcal{L}_2(x) - (1-x)^{2p}\mathcal{L}_2\big(x/(x-1)\big) \pmod{p}.$$

Using $\mathcal{L}_2(y) = y^p\mathcal{L}_2(1/y)$ with $y = x/(x-1)$, and rearranging terms, we obtain Eq. (6). Substituting it appropriately in Eq. (16) yields Eq. (14). □

We will follow a similar approach to prove Eq. (15). However, in this case Lemma 3.2 provides us with just about one third of the values modulo p of the coefficients of $\mathcal{L}_1(x)^3$, and so we need a more careful application of symmetries to recover the rest of the coefficients. For this reason we take some time to discuss the group of symmetries in some detail, and the polynomials which it leaves invariant.

If F is any field, the involutive transformations $R : z \mapsto 1/z$ and $S : z \mapsto 1-z$ of the projective line $F \cup \{\infty\}$ generate a group

$$G = \{1, R, S, RS, SR, RSR\} \tag{17}$$

of order six, which is isomorphic to the symmetric group on three objects (with 1 denoting the identity map). Thus, writing composition of maps from right to left, the group also contains the two elements $RS : z \mapsto 1/(1-z)$ and $SR : z \mapsto 1-1/z$, which have order three and are inverse of each other, and a third involution $RSR = SRS : z \mapsto z/(z-1)$. As is well known, $R^2 = 1$, $S^2 = 1$ and $RSR = SRS$ are a set of defining relations for G as a group generated by R and S.

The group G plays a crucial role in virtually all of this paper. By considering the fixed points of the various elements of G in the action it is easy to see that all orbits of G on $F \cup \{\infty\}$ have length six, with the only exceptions of the orbits $\{1, 0, \infty\}$ and $\{-1, 2, 1/2\}$ of length three (but they coincide if F has characteristic two, and the latter orbit has length one if F has characteristic three) and, possibly, an orbit $\{\omega_6, \omega_6^{-1}\}$ of length two (or one if F has characteristic three). This last orbit exists when F contains a root ω_6 of the polynomial $x^2 - x + 1$ (which for the finite field $F = \mathbb{F}_q$ is the case if and only if $q \equiv 0, 1 \pmod 3$).

This action of G on the projective line $F \cup \{\infty\}$ naturally induces an action on its function field as an algebraic variety. A formal treatment would require dealing with homogeneous polynomials and then rational functions in two indeterminates x_0 and x_1, but to avoid losing sight of the main argument we prefer to use the affine parameter $x = x_1/x_0$ for the projective line, at the expense of adding some *ad-hoc* terminology concerning the point ∞. (A few comments on the more formal point of view will be added in parentheses for the more algebraically-inclined reader.)

We define a linear representation of G on $F[x]_{\leqslant m}$, the space of polynomials of degree not exceeding m, by setting

$$(Rf)(x) := (-x)^m f(1/x) \quad \text{and} \quad (Sf)(x) := f(1-x),$$

for $f \in \mathbb{F}_p[x]_{\leqslant m}$. That this stipulation really defines a representation of G can be verified by checking that $R(Rf) = f$, $S(Sf) = f$, and $R(S(Rf)) = S(R(Sf))$. One finds

$$\begin{aligned}(RSf)(x) &= (-x)^m f(1-1/x),\\ (SRf)(x) &= (x-1)^m f\big(1/(1-x)\big),\\ (RSRf)(x) &= (x-1)^m f\big(x/(x-1)\big) = (SRSf)(x).\end{aligned}$$

(In terms of homogeneous coordinates (x_0, x_1) with $x = x_1/x_0$, we would obtain this representation of G on $F[x_0, x_1]$ by letting G act on a linear form $f(x_0, x_1) = x_0 f(1, x_1/x_0)$ by $(Rf)(x_0, x_1) := f(-x_1, -x_0)$ and $(Sf)(x_0, x_1) := f(x_0, x_0 - x_1)$.)

Given a polynomial $f \in F[x]$, we may assign to it a *formal degree* m, any integer no less than the ordinary degree $\deg f$, to indicate that we are viewing f as an element of $F[x]_{\leqslant m}$ and elements of the group G should act on it as described above. (Thus, the same polynomial can be assigned different formal degrees.) Then the action above is compatible with polynomial multiplication, in the sense that if f_1 and f_2 are polynomials of formal degrees m_1 and m_2, and we assign formal degree $m_1 + m_2$ to their product $f_1 f_2$, then $T(f_1 f_2) = (Tf_1)(Tf_2)$ for any $T \in G$. (This artifice makes up for not using homogeneous coordinates, and a polynomial of formal degree m really corresponds to a polynomial function of degree m on the projective line.) If we agree to say that a polynomial f of formal degree m has the point ∞ as a zero with multiplicity $m - \deg f$, then the sum of the multiplicities of the roots of f, including that of ∞, does not exceed its formal degree m, unless f is the zero polynomial.

If the field F has characteristic greater than 3, as we assume from now on, it is a basic fact that the map $f \mapsto (1/|G|) \sum_{T \in G} Tf$ projects $F[x]_{\leqslant m}$, the space of polynomials of formal degree m, onto its subspace of G-invariant polynomials. (This is the projection operator used in the standard proof of Maschke's theorem in the basic representation theory of finite groups, for example.) Thus, any G-invariant polynomial of formal degree m can be expressed as $f + Rf + Sf + RSf + SRf + RSRf$ for some $f \in F[x]_{\leqslant m}$. More conveniently for us, any G-invariant polynomial of formal degree m can be expressed as

$$(f + Sf + RSf)(x) = f(x) + f(1 - x) + (-x)^m f(1 - 1/x) \tag{18}$$

for some $f \in F[x]_{\leqslant m}$ with the extra property that $Rf = f$.

We are now getting close to a proof of congruence (15). The fact that most orbits of G on $F \cup \{\infty\}$ have length six implies that, roughly speaking, all the coefficients of a G-invariant polynomial f of formal degree m can be recovered from knowledge of only about $m/6$ coefficients, if carefully selected. Of course we will need to specify a larger number of coefficients if our selection encodes redundant information. The following lemma shows that the lower third of the coefficient list is a sufficiently large selection to this purpose.

Lemma 3.3. *Let f be a G-invariant polynomial of formal degree m. If f has no terms of degree $\leqslant m/3$, then f is the zero polynomial.*

Proof. By hypothesis 0 is a root of f with multiplicity strictly higher than $m/3$. Recall that the G-orbit of 0 is $\{0, 1, \infty\}$. Invariance under G implies that 1 and ∞ are also roots of f, each with multiplicity exceeding $m/3$. It follows that f is the zero polynomial. □

Lemma 3.4. *Let f be a polynomial with $\deg f < p$, over a field of characteristic $p > 3$, satisfying $f(x) = -x^p f(1/x)$. Then there is a unique G-invariant polynomial of formal degree $3p$ such that $g(x) \equiv f(1 - x) \pmod{x^{p+1}}$, and is given by*

$$g(x) = x^p f(x) + \left(1 - x^p\right) f(1 - x) + x^{2p}\left(1 - x^p\right) f(1 - 1/x).$$

Proof. That g is G-invariant follows by direct verification, or from a previous observation (namely, by taking $x^p f(x)$ in place of f in Eq. (18)).

Our hypotheses on f imply that both 0 and 1 are roots of f (as well as ∞ if we assign f formal degree p), and so $f(x)$, $f(1 - x)$ and $x^p f(1 - 1/x)$ are all polynomials of ordinary degree less than p and without constant term. It follows that $g(x) \equiv f(1 - x) \pmod{x^{p+1}}$.

Finally, uniqueness of f follows from Lemma 3.3. □

Proof of Eq. (15). According to Lemma 3.2 and [27, Corollary 2.3] (with $a = 3$), the polynomial

$$g(x) = \mathcal{L}_1(x)^3/6 - (2/3)x^p\left(1 - x^p\right)\mathcal{L}_3(-1)$$

satisfies the hypotheses of Lemma 3.4 with $f(x) = \mathcal{L}_3(x)$. □

4. Special values of $\mathcal{L}_d(x)$

In this section we collect several known congruences for special values of the finite polylogarithms $\mathcal{L}_d(x)$, and use the identities for finite polylogarithms from Section 2 to prove some new ones.

Let $B_n(x)$, $B_n = B_n(0)$ and E_n denote the Bernoulli polynomials, and the Bernoulli and Euler numbers. Note that $\mathcal{L}_d(1) = H_{p-1}(d)$, where $H_k(d) = \sum_{r=1}^{k} 1/r^d$. For any prime $p > d+2$ we have

$$\mathcal{L}_d(1) \equiv \begin{cases} -\frac{d(d+1)}{2(d+2)} p^2 B_{p-d-2} \pmod{p^3} & \text{if } d \text{ is odd,} \\ \frac{d}{d+1} p B_{p-d-1} \pmod{p^2} & \text{if } d \text{ is even.} \end{cases}$$

In essence these were found by Glaisher in 1900 in his articles in Quart. J. Math., but see [18, Theorem 5.1] for a sharper result.

To compute $\mathcal{L}_d(-1) = -H_{p-1}(d) + 2^{1-d} H_{(p-1)/2}(d)$, we combine the above congruences with the evaluation of $H_{(p-1)/2}(d)$ given in [18, Theorem 5.2]. For $d = 1$ we find, for any prime $p > 3$, the congruence

$$\mathcal{L}_1(-1) \equiv -2q_p(2) + pq_p^2(2) - p^2\left(\frac{2}{3}q_p^3(2) + \frac{1}{4}B_{p-3}\right) \pmod{p^3};$$

for $d > 1$, as soon as $p > d+1$, we obtain (see [27, Corollary 2.3])

$$\mathcal{L}_d(-1) \equiv \begin{cases} -\frac{2(1-2^{1-d})}{d} B_{p-d} \pmod{p} & \text{if } d \text{ is odd,} \\ \frac{d(1-2^{-d})}{(d+1)} p B_{p-d-1} \pmod{p^2} & \text{if } d \text{ is even.} \end{cases}$$

From [20, Theorem 4.1] and Eq. (4) we obtain congruences for $\mathcal{L}_d(2)$ and $\mathcal{L}_d(1/2)$, all valid for $p > 3$:

$$\begin{aligned}
\mathcal{L}_1(2) &\equiv -2q_p(2) - \frac{7}{12}p^2 B_{p-3} \pmod{p^3}, \\
\mathcal{L}_2(2) &\equiv -q_p^2(2) + p\left(\frac{2}{3}q_p^3(2) + \frac{7}{6}B_{p-3}\right) \pmod{p^2}, \\
\mathcal{L}_3(2) &\equiv -\frac{1}{3}q_p^3(2) - \frac{7}{24}B_{p-3} \pmod{p}, \\
\mathcal{L}_1(1/2) &\equiv q_p(2) - \frac{1}{2}pq_p^2(2) + p^2\left(\frac{1}{3}q_p^3(2) - \frac{7}{48}B_{p-3}\right) \pmod{p^3}, \\
\mathcal{L}_2(1/2) &\equiv -\frac{1}{2}q_p^2(2) + p\left(\frac{1}{2}q_p^3(2) + \frac{7}{24}B_{p-3}\right) \pmod{p^2}, \\
\mathcal{L}_3(1/2) &\equiv \frac{1}{6}q_p^3(2) + \frac{7}{48}B_{p-3} \pmod{p}.
\end{aligned}$$

The above evaluation of $\mathcal{L}_3(2)$ appears also in [5].

Finally, according to [19, Corollary 2.1] combined with Fermat's little theorem, for $d \geqslant 1$ and $m, r \geqslant 0$ we have

$$\sum_{\substack{0<k<p \\ k \equiv r \pmod m}} \frac{1}{k^d} \equiv \frac{1}{dm^d}\left(B_{p-d}\left(\left\{\frac{r}{m}\right\}\right) - B_{p-d}\left(\left\{\frac{r-p}{m}\right\}\right)\right) \pmod{p},$$

provided the prime p satisfies $p > d+3$ and $p \nmid m$, where $\{x\} = x - \lfloor x \rfloor$ is the fractional part of x. The above relation can be used to compute $\mathcal{L}_d(x)$ modulo p where x is an m-th root of unity. In particular, one finds that

$$\mathcal{L}_2(\pm i) \equiv \frac{1}{16}\left(\left(\frac{-1}{p}\right) \pm i\right) B_{p-2}(1/4) = \frac{1}{2}\left(\left(\frac{-1}{p}\right) \pm i\right) E_{p-3} \pmod p,$$
$$\mathcal{L}_3(\pm i) \equiv \frac{1}{32}\left(-1 \pm \left(\frac{-1}{p}\right) i\right) B_{p-3} \pmod p,$$

and

$$\mathcal{L}_2\big(\omega_6^{\pm 1}\big) \equiv \frac{1}{8}\left(\left(\frac{p}{3}\right) \pm i\frac{\sqrt{3}}{3}\right) B_{p-2}(1/3), \qquad \mathcal{L}_2\big(-\omega_6^{\pm 1}\big) \equiv \frac{1}{12}\left(\left(\frac{p}{3}\right) \mp i\sqrt{3}\right) B_{p-2}(1/3),$$
$$\mathcal{L}_3\big(\omega_6^{\pm 1}\big) \equiv \frac{1}{18}\left(1 \mp i\sqrt{3}\left(\frac{p}{3}\right)\right) B_{p-3}, \qquad \mathcal{L}_3\big(-\omega_6^{\pm 1}\big) \equiv \frac{2}{9}\left(-1 \mp i\frac{\sqrt{3}}{3}\left(\frac{p}{3}\right)\right) B_{p-3},$$

all four congruences being modulo p.

After recalling these known evaluations, we put to good use the group of transformations G which we introduced in Section 3, Eq. (17). Recall that its orbits on any field F have all length six, with the only exceptions of $\{1, 0, \infty\}$, $\{-1, 2, 1/2\}$, and possibly $\{\omega_6, \omega_6^{-1}\}$ if the field contains a root ω_6 of the polynomial $x^2 - x + 1$. We now consider three particular orbits of length six, namely

$$\big\{i, -i, 1+i, 1-i, (1+i)/2, (1-i)/2\big\},$$
$$\big\{-\omega_6, -\omega_6^{-1}, 1+\omega_6, 1+\omega_6^{-1}, (1+\omega_6)/3, \big(1+\omega_6^{-1}\big)/3\big\},$$
$$\big\{\phi_+, \phi_-, \phi_+^2, \phi_-^2, -\phi_+, -\phi_-\big\},$$

where $\phi_\pm = (1 \pm \sqrt{5})/2$ are the roots of the polynomial $x^2 - x - 1$. For each of these orbits the congruences given in Eqs. (3)–(8) provide several linear relations among the values modulo p of $\mathcal{L}_2(\alpha)$ with α ranging over the orbit. In the first two cases this will allow us to recover all those values from just one which is available from the literature, and in the third case the relations alone are sufficient to determine all those values. At this point we need the following lemma.

Lemma 4.1. *Let p be an odd prime and let a be an integer not divisible by p. Then*

$$\left(\frac{a}{p}\right) a^{(p-1)/2} \equiv \sum_{k=0}^{n-1} \binom{1/2}{k} \big(p q_p(a)\big)^k \pmod{p^n}$$

for any positive integer n.

Proof. The assertion, whose special case $n = 1$ is familiar, follows from the fact that

$$\left(\frac{a}{p}\right) a^{(p-1)/2} = \sum_{k=0}^{\infty} \binom{1/2}{k} \big(p q_p(a)\big)^k$$

in the ring of p-adic integers $\mathbb{Z}_p$. The latter is true because both sides are square roots of the integer $a^{p-1} = 1 + p q_p(a)$ in $\mathbb{Z}_p$, and both are congruent to 1 modulo p. □

Theorem 4.2. *For any prime $p > 3$ we have*

$$\mathcal{L}_2(1\pm i) \equiv -\frac{q_p^2(2)}{8}\left(1 \pm i\left(\frac{-1}{p}\right)\right) + \frac{1}{2}\left(\frac{-1}{p}\right)E_{p-3} \pmod p,$$

$$\mathcal{L}_2\big((1\pm i)/2\big) \equiv -\frac{q_p^2(2)}{8} + \frac{1}{4}\left(\left(\frac{-1}{p}\right) \pm i\right)E_{p-3} \pmod p.$$

Proof. We first compute $\mathcal{L}_2(1\pm i) = a \pm ib$, from which the remaining values can be obtained by means of the inversion relation (3). According to [20, Theorem 3.2] we have

$$\begin{aligned}\operatorname{Re}\big(\mathcal{L}_1(i)\big) &= \sum_{k=1}^{\lfloor p/4\rfloor}\frac{1}{4k} - \sum_{k=1}^{\lfloor p/4\rfloor}\frac{1}{4k-2} = \frac{1}{2}\sum_{k=1}^{\lfloor p/4\rfloor}\frac{1}{k} - \frac{1}{2}\sum_{k=1}^{\lfloor p/2\rfloor}\frac{1}{k}\\ &\equiv -\frac{1}{2}q_p(2) + \frac{1}{4}pq_p^2(2) - \frac{1}{2}p\left(\frac{-1}{p}\right)E_{p-3} \pmod{p^2}.\end{aligned}$$

Because

$$(1\pm i)^n = (-1)^{(n^2-1)/8}2^{(n-1)/2}\big(1 \pm (-1)^{(n-1)/2}i\big)$$

for n odd, Lemma 4.1 implies

$$\begin{aligned}\operatorname{Re}\big(Q_p(1-i)\big) &= \frac{\operatorname{Re}((1-i)^p) - 1}{p} = \frac{(\frac{2}{p})2^{(p-1)/2} - 1}{p}\\ &\equiv \frac{1}{2}q_p(2) - \frac{1}{8}pq_p^2(2) \pmod{p^2}.\end{aligned}$$

Using Eq. (7) we find

$$\operatorname{Re}\big(Q_p(1-i)\big) \equiv -\operatorname{Re}\big(\mathcal{L}_1(i)\big) - pa \pmod{p^2},$$

which allows us to determine a. Finally, Eq. (6) implies

$$\frac{1}{2}\left(\frac{-1}{p}\right)E_{p-3} \equiv \operatorname{Re}\big(\mathcal{L}_2(i)\big) \equiv \operatorname{Re}\big(a - ib + i^p(a+ib)\big) \equiv a - \left(\frac{-1}{p}\right)b \pmod p,$$

which yields b. □

Theorem 4.3. *For any prime $p > 3$ we have*

$$\mathcal{L}_2\big(1+\omega_6^{\pm1}\big) \equiv -\frac{q_p^2(3)}{16}\left(3 \pm i\sqrt{3}\left(\frac{p}{3}\right)\right) + \frac{1}{36}\left(3\left(\frac{p}{3}\right) \mp i\sqrt{3}\right)B_{p-2}(1/3) \pmod p,$$

$$\mathcal{L}_2\big(\big(1+\omega_6^{\pm1}\big)/3\big) \equiv -\frac{q_p^2(3)}{8} + \frac{1}{36}\left(\left(\frac{p}{3}\right) \pm i\sqrt{3}\right)B_{p-2}(1/3) \pmod p.$$

Proof. We compute $\mathcal{L}_2(1+\omega_6^{\pm 1}) = a \pm ib$, and the other congruence will follow from the inversion relation (3). From [20, Theorem 3.9] we have

$$\begin{aligned}\operatorname{Re}\bigl(\mathcal{L}_1(-\omega_6)\bigr) &= \frac{3}{2}\sum_{k=1}^{\lfloor p/3\rfloor}\frac{1}{3k} - \frac{1}{2}\sum_{k=1}^{p-1}\frac{1}{k} \\ &\equiv -\frac{3}{4}q_p(3) + \frac{3}{8}pq_p^2(3) - \frac{1}{12}p\left(\frac{p}{3}\right)B_{p-2}(1/3) \pmod{p^2}.\end{aligned}$$

Because

$$\omega_6^{\pm n} = \frac{(-1)^{n-1}}{2}\left(1 \pm i\sqrt{3}\left(\frac{n}{3}\right)\right)$$

if n is not a multiple of 3, Lemma 4.1 implies

$$\begin{aligned}\operatorname{Re}\bigl(Q_p(1+\omega_6)\bigr) &= \frac{\operatorname{Re}((\sqrt{3}i\omega_6^{-1})^p) - \operatorname{Re}(\omega_6^p) - 1}{p} = \frac{3}{2}\frac{(\frac{3}{p})3^{(p-1)/2} - 1}{p} \\ &\equiv \frac{3}{4}q_p(3) - \frac{3}{16}pq_p^2(3) \pmod{p^2}.\end{aligned}$$

Using Eq. (7) we find

$$\operatorname{Re}\bigl(Q_p(1+\omega_6)\bigr) \equiv -\operatorname{Re}\bigl(\mathcal{L}_1(-\omega_6)\bigr) - pa \pmod{p^2},$$

from which we can determine a. Finally, Eq. (6) implies

$$\begin{aligned}\frac{1}{12}\left(\frac{p}{3}\right)B_{p-2}(1/3) &\equiv \operatorname{Re}\bigl(\mathcal{L}_2(-\omega_6)\bigr) \equiv \operatorname{Re}\bigl(a + ib - \omega_6^p(a-ib)\bigr) \\ &\equiv \frac{1}{2}\left(a - \sqrt{3}\left(\frac{p}{3}\right)b\right) \pmod{p},\end{aligned}$$

which yields b. □

Theorem 4.4. *For any prime $p > 5$ we have*

$$\begin{aligned}\mathcal{L}_2(\phi_\pm) &\equiv \mp\frac{\sqrt{5}}{10}\left(\frac{p}{5}\right)q_L^2 \pmod{p}, \\ \mathcal{L}_2\bigl(\phi_\pm^2\bigr) &\equiv -\frac{1}{2}\left(1 \pm \frac{\sqrt{5}}{5}\left(\frac{p}{5}\right)\right)q_L^2 \pmod{p}, \\ \mathcal{L}_2(-\phi_\pm) &\equiv -\frac{1}{4}\left(1 \pm \frac{\sqrt{5}}{5}\left(\frac{p}{5}\right)\right)q_L^2 \pmod{p},\end{aligned}$$

where $q_L = Q_p(\phi_\pm) = (L_p - 1)/p$ is the Lucas quotient. *Moreover, we have*

$$\mathcal{L}_3\bigl(\phi_\pm^2\bigr) \equiv -\frac{2}{15}\left(1 \pm \sqrt{5}\left(\frac{p}{5}\right)\right)\left(\frac{1}{2}q_L^3 + B_{p-3}\right) \pmod{p}.$$

Proof. The distribution relation (5) with $m = 2$ and $d = 2$ yields

$$\mathcal{L}_2\big(\phi_+^2\big) \equiv 2\phi_+^{2p}\mathcal{L}_2(\phi_+) + 2\phi_+^p\mathcal{L}_2(-\phi_+) \pmod p.$$

Eq. (6) and the inversion relation (3) yield

$$\mathcal{L}_2\big(\phi_+^2\big) - \mathcal{L}_2(-\phi_+) \equiv \phi_+^{2p}\mathcal{L}_2(-\phi_-) \equiv \phi_+^p\mathcal{L}_2(\phi_+) \pmod p.$$

Eq. (8) and the inversion relation (3) yield

$$\frac{1}{2}q_L^2 + \phi_+^p\mathcal{L}_2(\phi_+) \equiv -\phi_-^p\mathcal{L}_2(\phi_-) \equiv -\phi_-^{2p}\mathcal{L}_2(-\phi_+) \pmod p.$$

Solving the linear system for $\mathcal{L}_2(\phi_+)$, $\mathcal{L}_2(\phi_+^2)$ and $\mathcal{L}_2(-\phi_+)$ given by the above three congruences, and using

$$2\phi_\pm^p \equiv \left(1 \pm \sqrt{5}\left(\frac{p}{5}\right)\right) \quad \text{and} \quad 2\phi_\pm^{2p} \equiv \left(3 \pm \sqrt{5}\left(\frac{p}{5}\right)\right) \pmod p,$$

one obtains the three stated congruences involving $\mathcal{L}_2$.

In a similar way one evaluates $\mathcal{L}_2$ and $\mathcal{L}_3$ at $\phi_\pm^2$. The distribution relation (5), with $m = 2$ and $d = 3$, combined with the inversion relation (3), yields

$$\mathcal{L}_3\big(\phi_+^2\big) - 4\phi_+^{2p}\mathcal{L}_3(\phi_+) \equiv -4\mathcal{L}_3(\phi_-) \pmod p.$$

Also, congruence (9) yields

$$\frac{1}{6}q_L^3 + \frac{1}{3}B_{p-3} \equiv -\phi_-^p\mathcal{L}_3(\phi_-) - \phi_+^p\mathcal{L}_3(\phi_+) + \phi_-^p\mathcal{L}_3\big(\phi_+^2\big) \pmod p.$$

Solving for $\mathcal{L}_3(\phi_+^2)$ we find

$$\mathcal{L}_3\big(\phi_+^2\big) \equiv -\frac{4\phi_+^p}{15}\left(\frac{1}{2}q_L^3 + B_{p-3}\right) \equiv -\frac{2}{15}\left(1 + \sqrt{5}\left(\frac{p}{5}\right)\right)\left(\frac{1}{2}q_L^3 + B_{p-3}\right) \pmod p.$$

The analogous congruence for $\mathcal{L}_3(\phi_-^2)$ is obtained by interchanging the subscripts $+$ and $-$ throughout the proof. □

5. Polynomial identities

The main goal of this section, which we achieve in Theorem 5.2, is to obtain identities which allow one to replace the two general partial sums $\sum_{k=1}^n k^{-s}\binom{2k}{k}^{-1}t^k$, with $s = 1, 2, 3$ (and also higher, in principle), with more manageable sums. Those involve the familiar Lucas sequences $\{u_n(x)\}_{n\geqslant 0}$ and $\{v_n(x)\}_{n\geqslant 0}$ defined by the recurrence relations

$$u_0(x) = 0, \qquad u_1(x) = 1, \quad \text{and} \quad u_n(x) = xu_{n-1}(x) - u_{n-2}(x) \quad \text{for } n > 1,$$
$$v_0(x) = 2, \qquad v_1(x) = x, \quad \text{and} \quad v_n(x) = xv_{n-1}(x) - v_{n-2}(x) \quad \text{for } n > 1.$$

They have generating functions

$$U(z) = \sum_{n\geqslant 0} u_n(x) z^n = \frac{z}{1 - xz + z^2} \quad \text{and} \quad V(z) = \sum_{n\geqslant 0} v_n(x) z^n = \frac{2 - xz}{1 - xz + z^2},$$

where we have omitted the dependence of $U(z)$ and $V(z)$ on x in favor of a lighter notation. It is convenient to view x as an indeterminate rather than a specific number. Thus, letting α be an element of a quadratic field extension of the field $\mathbb{Q}(x)$ of rational functions with $\alpha^2 - x\alpha + 1 = 0$, we have $u_n(x) = (\alpha^n - \alpha^{-n})/(\alpha - \alpha^{-1})$ and $v_n(x) = \alpha^n + \alpha^{-n}$. We anticipate that in Section 6 we will obtain polynomial congruences, relative to a prime p, which involve sums of the form $\sum_{k=1}^{p-1} u_k(x)/k^d = (\mathcal{L}_d(\alpha) - \mathcal{L}_d(\alpha^{-1}))/(\alpha - \alpha^{-1})$ and $\sum_{k=1}^{p-1} v_k(x)/k^d = \mathcal{L}_d(\alpha) + \mathcal{L}_d(\alpha^{-1})$. Thus, specializations of those polynomial congruences to numerical congruences will follow from knowledge of special values of finite polylogarithms which we have obtained in Section 4, as we will illustrate in our final Section 8.

Note that $u_{n+1}(x)$ and $v_n(x)$ are even polynomials if n is even, and odd polynomials otherwise. Some readers of different backgrounds may recognize them as related to the classical Chebyshev polynomials of the first and second kind $T_n(x)$ and $U_n(x)$, or to their (renormalized) generalizations known as Dickson polynomials $D_n(x,\alpha)$ and $E_n(x,\alpha)$. In fact,

$$u_{n+1}(x) = E_n(x,1) = U_n(x/2) \quad \text{and} \quad v_n(x) = D_n(x,1) = 2T_n(x/2).$$

The same readers may be aware that $(d/dx)T_n(x) = nU_{n-1}(x)$ for $n > 0$, which becomes $(d/dx)v_n(x) = nu_n(x)$ here. Besides recalling this fact in an integral formulation which is more suitable for us, the following preliminary result provides us with an expression for a primitive of the polynomial $(v_n(x) - v_n(-2))/(x+2)$.

Lemma 5.1. *For any $n > 0$ we have*

$$\int_0^t u_n(\tau - 2)\, d\tau = \frac{v_n(t-2) - 2(-1)^n}{n}, \tag{19}$$

$$\int_0^t \frac{v_n(\tau-2) - 2(-1)^n}{\tau}\, d\tau = \frac{v_n(t-2) - 2(-1)^n}{n} + 2\sum_{k=1}^{n-1} (-1)^{n-k} \frac{v_k(t-2) - 2(-1)^k}{k}. \tag{20}$$

Proof. Temporarily viewing x as a complex constant and working in the formal power series ring $\mathbb{C}[[z]]$, write $z^2 - xz + 1 = (1 - \alpha z)(1 - \beta z)$. Then $V(z) = (1 - \alpha z)^{-1} + (1 - \beta z)^{-1}$, and so for $n > 0$ we have

$$\big[z^n\big] \log\big(z^2 - xz + 1\big) = \big[z^n\big]\big(\log(1 - \alpha z) + \log(1 - \beta z)\big) = -\big(\alpha^n + \beta^n\big)/n = -v_n(x)/n.$$

Using this and setting $x = \tau - 2$ we obtain

$$\begin{aligned}\int_0^t u_n(\tau - 2)\, d\tau &= \big[z^n\big] \int_0^t U(z)\, d\tau \\ &= \big[z^n\big]\big(-\log\big(z^2 - (t-2)z + 1\big) + 2\log(1+z)\big) = \frac{v_n(t-2) - 2(-1)^n}{n}.\end{aligned}$$

Similarly, but with a slightly more complicated integrand, we obtain

$$\int_0^t \frac{v_n(\tau-2)-2(-1)^n}{\tau}\,d\tau = \bigl[z^n\bigr]\int_0^t \left(V(z)-\frac{2}{1+z}\right)\frac{d\tau}{\tau}$$
$$= \bigl[z^n\bigr]\left(\bigl(-\log\bigl(z^2-(t-2)z+1\bigr)+2\log(1+z)\bigr)\cdot\frac{1-z}{1+z}\right)$$
$$= \frac{v_n(t-2)-2(-1)^n}{n}+2\sum_{k=1}^{n-1}(-1)^{n-k}\frac{v_k(t-2)-2(-1)^k}{k},$$

where we have expanded $(1-z)/(1+z)=1-2z/(1+z)=1+2\sum_{k>0}(-z)^k$ for the last passage. □

We are now ready to state the main result of this section, which expresses certain sums of the form $\sum_{k=1}^n k^{-s}\binom{2k}{k}^{-1}t^k$ in terms of other sums involving our Lucas sequences. The crucial case is Eq. (21), where $s=1$, from which the other equations will follow by integration using Lemma 5.1. The case $s=0$ excluded here may be obtained from Eq. (21) by differentiation, but we prefer to deal with it differently in Theorem 5.3.

Theorem 5.2. *For $n\geqslant 1$ we have the polynomial identities*

$$\binom{2n}{n}\sum_{k=1}^n \frac{t^{k-1}}{k\binom{2k}{k}} = \sum_{k=1}^n \binom{2n}{n-k}\frac{u_k(t-2)}{k}, \tag{21}$$

$$\binom{2n}{n}\sum_{k=1}^n \frac{t^{k}}{k^2\binom{2k}{k}} = \sum_{k=1}^n \binom{2n}{n-k}\frac{v_k(t-2)}{k^2}+\binom{2n}{n}\sum_{k=1}^n\frac{1}{k^2}, \tag{22}$$

$$\binom{2n}{n}\sum_{k=1}^n \frac{t^{k}}{k^3\binom{2k}{k}} = \sum_{k=1}^n \binom{2n}{n-k}\frac{v_k(t-2)}{k^3}$$
$$+2\sum_{1\leqslant j<k\leqslant n}\binom{2n}{n-k}\frac{(-1)^{k-j}v_j(t-2)}{jk^2}+\binom{2n}{n}\sum_{k=1}^n\frac{1}{k^3}. \tag{23}$$

Our proof of Eq. (21) involves a transformation of sequences given by

$$\bigl\{c(n)\bigr\}_{n\geqslant 1}\to\bigl\{s(n)\bigr\}_{n\geqslant 0},\quad \text{where } s(n)=\binom{2n}{n}\sum_{k=1}^n\frac{c(k)}{\binom{2k}{k}},$$

which we read as $s(0)=0$ for $n=0$. More generally, in the sequel we interpret a sum to vanish when the upper summation limit is one less than the lower summation limit. The resulting sequence $s(n)$ is related to the original sequence $c(n)$ by the recurrence

$$s(0)=0,\qquad \Delta_n\bigl(s(n)\bigr):=(n+1)s(n+1)-2(2n+1)s(n)=(n+1)c(n+1). \tag{24}$$

Proof of Theorem 5.2. We start with proving Eq. (21). Consider the sequence

$$a_d(n)=\binom{2n}{n}\sum_{k=1}^n\frac{t^{k-1}}{k^d\binom{2k}{k}},$$

and the corresponding generating function $A_d(z) = \sum_{n\geqslant 0} a_d(n)z^n$. When $d = 1$ we have

$$\begin{aligned}\bigl(A_1(z)\sqrt{1-4z}\bigr)' &= \sum_{n=0}^{\infty}\left(na_1(n)z^{n-1}\sqrt{1-4z} - \frac{2a_1(n)z^n}{\sqrt{1-4z}}\right)\\ &= \frac{1}{\sqrt{1-4z}}\sum_{n=0}^{\infty}\bigl(na_1(n)z^{n-1} - 4na_1(n)z^n - 2a_1(n)z^n\bigr)\\ &= \frac{1}{\sqrt{1-4z}}\left(\sum_{n=1}^{\infty}na_1(n)z^{n-1} - 2\sum_{n=0}^{\infty}(2n+1)a_1(n)z^n\right)\\ &= \frac{1}{\sqrt{1-4z}}\sum_{n=0}^{\infty}\bigl((n+1)a_1(n+1) - 2(2n+1)a_1(n)\bigr)z^n.\end{aligned}$$

According to Eq. (24) we have

$$\Delta_n\bigl(a_1(n)\bigr) = (n+1)a_1(n+1) - 2(2n+1)a_1(n) = t^n \quad \text{for } n \geqslant 0,$$

and so

$$\bigl(A_1(z)\sqrt{1-4z}\bigr)' = \frac{1}{\sqrt{1-4z}}\left(\sum_{n=0}^{\infty}(tz)^n\right) = \frac{1}{(1-tz)\sqrt{1-4z}}.$$

Now consider the sequence

$$b_1(n) = \sum_{k=1}^{\infty}\binom{2n}{n+k}\frac{u_k(t-2)}{k}.$$

Its generating function $B_1(z) = \sum_{n\geqslant 0} b_1(n)z^n$ is

$$\begin{aligned}B_1(z) &= \sum_{k=1}^{\infty}\frac{u_k(t-2)}{k}\sum_{n\geqslant 1}\binom{2n}{n+k}z^n\\ &= \sum_{k=1}^{\infty}\frac{u_k(t-2)}{k}\left(\frac{4z}{(1+\sqrt{1-4z})^2}\right)^k\frac{1}{\sqrt{1-4z}} = \frac{1}{\sqrt{1-4z}}U_1\bigl(h(z)\bigr),\end{aligned}$$

where

$$h(z) = \frac{4z}{(1+\sqrt{1-4z})^2} \quad \text{and} \quad U_d(z) = \sum_{k=1}^{\infty}\frac{u_k(t-2)z^k}{k^d}.$$

Because $z(d/dz)U_1 = U$, we deduce that

$$\bigl(B_1(z)\sqrt{1-4z}\bigr)' = \frac{d}{dz}U_1\bigl(h(z)\bigr) = \frac{h'(z)}{h(z)}U\bigl(h(z)\bigr) = \frac{1}{(1-tz)\sqrt{1-4z}}.$$

Finally, $A_1(0) = B_1(0)$ and $(A_1(z)\sqrt{1-4z})' = (B_1(z)\sqrt{1-4z})'$ imply that $A_1(z) = B_1(z)$, and we conclude that Eq. (21) holds.

To prove Eq. (22), integrate Eq. (21) with respect to t and then use Eq. (19), to obtain

$$\binom{2n}{n}\sum_{k=1}^{n}\frac{t^k}{k^2\binom{2k}{k}}=\sum_{k=1}^{n}\binom{2n}{n-k}\frac{v_k(t-2)-2(-1)^k}{k^2}$$
$$=\sum_{k=1}^{n}\binom{2n}{n-k}\frac{v_k(t-2)}{k^2}+\binom{2n}{n}\sum_{k=1}^{n}\frac{1}{k^2}.$$

One can prove Eq. (23) in a similar way, by integrating Eq. (22) divided by t and then using Eq. (20). □

Eq. (25) in the following result shows how the study of $\sum_{k=1}^{n}\binom{2k}{k}^{-1}t^k$ can be reduced to the sums considered in Theorem 5.2. Eq. (26) gives a similar formula for $\sum_{k=1}^{n}H_{k-1}(s)\binom{2k}{k}^{-1}t^k$ with $s>0$. Note that Eq. (26) would not specialize correctly to the case $s=0$, where $H_{k-1}(0)=k-1$, which instead may be obtained from Eq. (22) by differentiation if one wishes.

Theorem 5.3. *For any $n,s\geqslant 1$ we have the polynomial identities*

$$(t-4)\sum_{k=1}^{n}\frac{t^{k-1}}{\binom{2k}{k}}+2\sum_{k=1}^{n}\frac{t^{k-1}}{k\binom{2k}{k}}=\frac{t^n}{\binom{2n}{n}}-1, \tag{25}$$

$$(t-4)\sum_{k=1}^{n}\frac{t^{k-1}H_{k-1}(s)}{\binom{2k}{k}}+2\sum_{k=1}^{n}\frac{t^{k-1}H_{k-1}(s)}{k\binom{2k}{k}}=\frac{t^nH_n(s)}{\binom{2n}{n}}-\sum_{k=1}^{n}\frac{t^k}{k^s\binom{2k}{k}}. \tag{26}$$

Proof. With the same notation as in the proof of Theorem 5.2, Eq. (24) implies

$$\Delta_n\big((t-4)a_0(n)+2a_1(n)\big)=(t-4)(n+1)t^n+2t^n=\Delta_n\big(t^n\big)=\Delta_n\left(t^n-\binom{2n}{n}\right).$$

Because the two sequences agree on $n=0$, Eq. (25) follows.

To prove Eq. (26), consider

$$a_d^{(s)}(n)=\binom{2n}{n}\sum_{k=1}^{n}\frac{t^{k-1}H_{k-1}(s)}{k^d\binom{2k}{k}}.$$

Eq. (24) yields, for $n\geqslant 0$,

$$\Delta_n\big(a_d^{(s)}(n)\big)=\frac{t^nH_n(s)}{(n+1)^{d-1}}.$$

This implies

$$\Delta_n\big((t-4)a_0^{(s)}(n)+2a_1^{(s)}(n)\big)=(t-4)(n+1)t^nH_n(s)+2t^nH_n(s)$$
$$=\Delta_n\big(t^nH_n(s)\big)-\frac{t^{n+1}}{(n+1)^{s-1}}$$
$$=\Delta_n\big(t^nH_n(s)-ta_s(n)\big).$$

Because the two sequences agree on $n=0$, Eq. (26) follows. □

We point out that trigonometric versions of our Eqs. (21), (22) and (25), with $4\cos^2\varphi$ in place of t, have recently appeared in [29, Eqs. (1.1), (5.1) and (1.3)]. The proofs given there are essentially different from ours.

6. Polynomial congruences

In this section we specialize the two partial sums $\sum_{k=1}^{n} k^{-s}\binom{2k}{k}^{-1}t^k$, with $s=1,2$, considered in Theorem 5.2, by setting $n=p-1$, and study their values modulo p^2. (Note that the values of those sums become p-integral only upon multiplication by p.) Theorem 6.1 also contains similar but less sharp evaluations for the corresponding sums $\sum_{k=1}^{n} k^{-s}H_{k-1}(2)\binom{2k}{k}^{-1}t^k$. As we anticipated in the first paragraph of Section 5, the possibility of specializing these polynomial congruences to numerical congruences, exemplified in Section 8, depends on our knowledge of special values of finite polylogarithms which we have developed in Section 4.

Theorem 6.1. *For any prime $p>3$ we have the polynomial congruences*

$$p\sum_{k=1}^{p-1}\frac{t^k}{k\binom{2k}{k}}\equiv\frac{tu_p(2-t)-t^p}{2}+p^2t\sum_{k=1}^{p-1}\frac{u_k(2-t)}{k^2}\pmod{p^3}, \tag{27}$$

$$p\sum_{k=1}^{p-1}\frac{t^k}{k^2\binom{2k}{k}}\equiv\frac{2-v_p(2-t)-t^p}{2p}-p^2\sum_{k=1}^{p-1}\frac{v_k(2-t)}{k^3}\pmod{p^3}, \tag{28}$$

and also

$$p\sum_{k=1}^{p-1}\frac{t^kH_{k-1}(2)}{k\binom{2k}{k}}\equiv t\sum_{k=1}^{p-1}\frac{u_k(2-t)}{k^2}\pmod{p}, \tag{29}$$

$$p\sum_{k=1}^{p-1}\frac{t^kH_{k-1}(2)}{k^2\binom{2k}{k}}\equiv-\sum_{k=1}^{p-1}\frac{v_k(2-t)}{k^3}\pmod{p}. \tag{30}$$

Proof. Setting $n=p$ in Eq. (21) and multiplying by pt we obtain

$$p\binom{2p}{p}\sum_{k=1}^{p-1}\frac{t^k}{k\binom{2k}{k}}+t^p=tu_p(t-2)+pt\sum_{k=1}^{p-1}\binom{2p}{k}\frac{u_{p-k}(t-2)}{p-k}.$$

Now $\binom{2p}{k}=\frac{2p}{k}\binom{2p-1}{k-1}\equiv 2(-1)^{k-1}p/k \pmod{p^2}$ for $k=1,\dots,p-1$, and $\binom{2p}{p}\equiv 2-\frac{4}{3}p^3B_{p-3} \pmod{p^4}$ according to [30, Theorem 3.2]. Because $u_k(-x)=(-1)^{k-1}u_k(x)$, we deduce

$$\begin{aligned}2p\sum_{k=1}^{p-1}\frac{t^k}{k\binom{2k}{k}}+t^p&\equiv tu_p(t-2)+2p^2t\sum_{k=1}^{p-1}\frac{(-1)^{k-1}u_{p-k}(t-2)}{k(p-k)}\\&\equiv tu_p(2-t)+2p^2t\sum_{k=1}^{p-1}\frac{u_k(2-t)}{k^2}\pmod{p^3},\end{aligned}$$

which is equivalent to the desired Eq. (27).

To pass from this to Eq. (29) we need to relate the sums

$$\sum_{k=1}^{p-1} \frac{t^k}{k\binom{2k}{k}} \quad \text{and} \quad \sum_{k=1}^{p-1} \frac{t^k H_{k-1}(2)}{k\binom{2k}{k}}$$

via an appropriate congruence. To this purpose we need the former of the following identities, valid for $n \geqslant 1$, which were obtained by the second author in the course of the proof of [26, Theorem 3.1]:

$$\sum_{k=1}^{n} \binom{n}{k}\binom{n+k-1}{k-1} \frac{(-t)^{k-1}}{\binom{2k}{k}} = \frac{(-1)^{n-1} u_n(t-2)}{2}, \tag{31}$$

$$\sum_{k=0}^{n} \binom{n}{k}\binom{n+k-1}{k} \frac{(-t)^{k}}{\binom{2k}{k}} = \frac{(-1)^{n} v_n(t-2)}{2}. \tag{32}$$

The latter identity will be needed later to pass from Eq. (28) to Eq. (30). Note that the coefficient of $(-t)^{k-1}$ in the former formula, for example, may be more simply written as $\frac{1}{2}\binom{n+k-1}{2k-1}$, but here we need the longer form, with the factor $\binom{2k}{k}^{-1}$ in evidence.

Thus, setting $n = p$ in Eq. (31) and separating the last summand we obtain

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

One easily checks that for $k = 1, \ldots, p-1$ we have

$$\frac{k}{p}\binom{p}{k} = \binom{p-1}{k-1} \equiv (-1)^{k-1}\bigl(1 - pH_{k-1}(1) + p^2 H_{k-1}(1,1)\bigr) \pmod{p^3},$$

$$\binom{p-1+k}{k-1} \equiv 1 + pH_{k-1}(1) + p^2 H_{k-1}(1,1) \pmod{p^3},$$

whence

$$\begin{aligned}\binom{p}{k}\binom{p-1+k}{k-1} &\equiv (-1)^{k-1}\frac{p}{k}\bigl(1 - p^2\bigl(H_{k-1}(1)^2 - 2H_{k-1}(1,1)\bigr)\bigr) \\ &\equiv (-1)^{k-1}\frac{p}{k}\bigl(1 - p^2 H_{k-1}(2)\bigr) \pmod{p^4}. \end{aligned} \tag{33}$$

Noting that $\binom{2k}{k}$ can be a multiple of p but not of p^2 in the range considered, we obtain

$$p\sum_{k=1}^{p-1} \frac{t^k}{k\binom{2k}{k}} - p^3 \sum_{k=1}^{p-1} \frac{t^k H_{k-1}(2)}{k\binom{2k}{k}} \equiv \frac{t u_p(2-t) - t^p}{2} \pmod{p^3}.$$

Together with Eq. (27) this implies Eq. (29).

The proofs of Eqs. (28) and (30) are similar. Setting $n = p$ in Eq. (22) and multiplying by p we obtain

$$p\binom{2p}{p}\sum_{k=1}^{p-1}\frac{t^k}{k^2\binom{2k}{k}}+\frac{t^p}{p}=\frac{v_p(t-2)}{p}+p\sum_{k=1}^{p-1}\binom{2p}{k}\frac{v_{p-k}(t-2)}{(p-k)^2}+p\binom{2p}{p}H_{p-1}(2)+\frac{1}{p}\binom{2p}{p}.$$

Because $v_k(-x)=(-1)^k v_k(x)$ and $H_{p-1}(2)\equiv 0 \pmod p$, we have

$$2p\sum_{k=1}^{p-1}\frac{t^k}{k^2\binom{2k}{k}}\equiv\frac{2-v_p(t-2)-t^p}{p}+2p^2\sum_{k=1}^{p-1}\frac{(-1)^{k-1}v_{p-k}(t-2)}{k(p-k)^2}\equiv\frac{2-v_p(2-t)-t^p}{p}-2p^2\sum_{k=1}^{p-1}\frac{v_k(2-t)}{k^3}\pmod{p^3},$$

and hence Eq. (28) holds.

Setting $n=p$ in Eq. (32), dividing by p and separating the last summand we find

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

According to Eq. (33), in the range considered for k we have

$$\frac{1}{p}\binom{p}{k}\binom{p-1+k}{k}=\frac{1}{k}\binom{p}{k}\binom{p-1+k}{k-1}\equiv(-1)^{k-1}\frac{p}{k^2}\bigl(1-p^2H_{k-1}(2)\bigr)\pmod{p^4},$$

and because $\binom{2k}{k}$ is not a multiple of p^2 we conclude

$$p\sum_{k=1}^{p-1}\frac{t^k}{k^2\binom{2k}{k}}-p^3\sum_{k=1}^{p-1}\frac{t^kH_{k-1}(2)}{k^2\binom{2k}{k}}\equiv\frac{2-v_p(t-2)-t^p}{2p}\pmod{p^3}.$$

Together with Eq. (28) this implies Eq. (30). □

Theorem 6.1 has exploited only the first two of the three polynomial congruences produced in Theorem 5.2. The third congruence we can only use in a weakened form, obtaining the following result.

Theorem 6.2. *For any prime $p>3$ we have the polynomial congruence*

$$p\sum_{k=1}^{p-1}\frac{t^k}{k^3\binom{2k}{k}}\equiv\frac{1-(v_p(2-t)+t^p)\binom{2p}{p}^{-1}}{p^2}-\frac{1}{p}\sum_{k=1}^{p-1}\frac{v_k(2-t)}{k}\pmod{p^2}.$$

Proof. The proof runs along similar lines as that of Theorem 6.1, but starting from Eq. (23). □

7. Congruences with $\binom{2k}{k}$ in the numerators

In this section we prove polynomial identities and congruences for sums similar to those considered in the previous sections, but involving the central binomial coefficients $\binom{2k}{k}$ in the numerators rather than the denominators.

One can obtain polynomials identities analogous to those of Section 5 starting from the identity

$$\sum_{k=0}^{n-1}\binom{2k}{k}t^{n-1-k}=\sum_{k=1}^{n}\binom{2n}{n-k}u_k(t-2), \tag{34}$$

which was proved in [25]. In fact, successive integration according to Lemma 5.1 produces the polynomial identities

$$\sum_{k=0}^{n-1}\frac{\binom{2k}{k}}{n-k}t^{n-k}=\sum_{k=1}^{n}\binom{2n}{n-k}\frac{v_k(t-2)-2(-1)^k}{k}, \tag{35}$$

$$\begin{aligned}\sum_{k=0}^{n-1}\frac{\binom{2k}{k}}{(n-k)^2}t^{n-k}&=\sum_{k=1}^{n}\binom{2n}{n-k}\frac{v_k(t-2)-2(-1)^k}{k^2}\\&\quad+2\sum_{1\leqslant j<k\leqslant n}\binom{2n}{n-k}\frac{(-1)^{k-j}(v_j(t-2)-2(-1)^j)}{jk},\end{aligned} \tag{36}$$

which are somehow analogous to the first two identities in Theorem 5.2. Eq. (35) will play a role in deducing Eq. (42) from Eq. (41) in our proof of Theorem 7.1 below.

Passing now to polynomial congruences, a simple way of switching central binomial coefficients from denominators to numerators of our sums is based on the congruence

$$\frac{2p}{k\binom{2k}{k}}\equiv\binom{2(p-k)}{p-k}\pmod p,\quad\text{for } k=1,\dots,p-1.$$

Accordingly, Eqs. (29) and (30) of Theorem 6.1 have equivalent formulations

$$\sum_{k=1}^{p-1}t^{p-k}H_k(2)\binom{2k}{k}\equiv-2t\sum_{k=1}^{p-1}\frac{u_k(2-t)}{k^2}\pmod p, \tag{37}$$

$$\sum_{k=1}^{p-1}\frac{t^{p-k}H_k(2)}{k}\binom{2k}{k}\equiv-2\sum_{k=1}^{p-1}\frac{v_k(2-t)}{k^3}\pmod p. \tag{38}$$

However, because Eqs. (27) and (28) of Theorem 6.1 are congruences modulo p^3, this simple trick is insufficient to turn them into equivalent congruences with the central binomial coefficients in the numerators. To achieve that we need to work a bit harder, as in our next result.

Evaluations of $\sum_{k=0}^{p-1}\binom{2k}{k}t^{p-1-k}\pmod{p^2}$ and $\sum_{k=1}^{p-1}\binom{2k}{k}k^{-1}t^{p-k}\pmod p$ were obtained in [22, Eq. (2.2)] and [25, Eq. (1.11)], respectively, starting from Eq. (34) above, and the further polynomial identity

$$\sum_{k=1}^{n-1}\frac{\binom{2k}{k}}{k}t^{n-k}=-2\sum_{d=1}^{n-1}\frac{(-1)^d}{d}\sum_{k=0}^{n-d-1}\binom{2n}{k}v_{n-d-k}(t-2)-4\sum_{d=1}^{n-1}\frac{(-1)^d}{d}\binom{2n-1}{n-d-1}, \tag{39}$$

which was also proved in [25, Eqs. (2.2) and (4.1)]. The key to push those evaluations in [22,25] to higher moduli lies in some of the functional equations for the finite polylogarithms which we have recalled in Section 2. The resulting congruences involve the Lucas sequences

$$u_0(x,y)=0, \qquad u_1(x,y)=1, \quad \text{and} \quad u_n(x,y)=xu_{n-1}(x,y)-yu_{n-2}(x,y) \quad \text{for } n>1,$$
$$v_0(x,y)=2, \qquad v_1(x,y)=x, \quad \text{and} \quad v_n(x,y)=xv_{n-1}(x,y)-yv_{n-2}(x,y) \quad \text{for } n>1,$$

which generalize the Lucas sequences $u_n(x)=u_n(x,1)$ and $v_n(x)=v_n(x,1)$ introduced in Section 5. Once again, letting α be an element of a quadratic field extension of the field $\mathbb{Q}(x,y)$ of rational functions with $\alpha^2-x\alpha+y=0$, we have $u_n(x)=(\alpha^n-\alpha^{-n})/(\alpha-\alpha^{-1})$ and $v_n(x)=\alpha^n+\alpha^{-n}$.

Theorem 7.1. *For any prime $p>3$ we have the polynomial congruences*

$$\sum_{k=0}^{p-1}\binom{2k}{k}t^{p-1-k}\equiv 2u_p(t,t)-u_p(2-t)-2p^2\sum_{k=1}^{p-1}\frac{u_k(2-t)+u_k(t,t)}{k^2} \pmod{p^3}, \tag{40}$$

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k}t^{p-k}\equiv\frac{3t^p+2-v_p(2-t)-4v_p(t,t)}{p} \pmod{p^2}, \tag{41}$$

$$\frac{1}{2}\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k^2}t^{p-k}\equiv\frac{v_p(2-t)+2v_p(t,t)-t^p-2}{p^2}+\sum_{k=1}^{p-1}\frac{v_k(2-t)}{k^2} \pmod{p}. \tag{42}$$

Note that if α is an element of a quadratic field extension of the field $\mathbb{Q}(t)$ of rational functions with $\alpha^2-(2-t)\alpha+1=0$, whence $u_n(2-t)=(\alpha^n-\alpha^{-n})/(\alpha-\alpha^{-1})$ and $v_n(2-t)=\alpha^n+\alpha^{-n}$, then $1-\alpha$ satisfies $(1-\alpha)^2-t(1-\alpha)+t=0$, whence $u_n(t,t)=((1-\alpha)^n-(1-\alpha^{-1})^n)/(\alpha^{-1}-\alpha)$ and $v_n(t,t)=(1-\alpha)^n+(1-\alpha^{-1})^n$. Consequently, the sum in the right-hand side of Eq. (40) can be expressed in terms of $\mathcal{L}_2(\alpha^{\pm1})$ and $\mathcal{L}_2(1-\alpha^{\pm1})$. Because the proof of Theorem 7.1 is very similar to that of Theorem 6.1, we only outline the argument.

Sketch of proof. The general scheme of proof is to deduce the congruences (40) and (41) from the identities (34) and (39) in a similar way as we deduced the congruences (27) and (28) of Theorem 6.1 from the identities (21) and (22) of Theorem 5.2. Thus, after taking $n=p$ and separating one term of the sum we apply standard congruences for binomial coefficients, but modulo a higher power of p than those needed in the proof of Theorem 6.1, such as

$$\binom{2p}{k}\equiv(-1)^{k-1}\frac{2p}{k}\bigl(1-2pH_{k-1}(1)\bigr) \pmod{p^3}, \quad \text{for } k=1,\dots,p-1.$$

Because $H_{p-k-1}(1)\equiv H_{k-1}(1)+1/k \pmod{p}$, the effect of this higher precision is the appearance of new terms, such as $p^2\sum_{k=1}^{p-1}u(2-t,1)/k^2=p^2(\mathcal{L}_2(\alpha)-\mathcal{L}_2(\alpha^{-1}))/(\alpha-\alpha^{-1})$, in contrast with the proof of Theorem 6.1, which only involved $\mathcal{L}_1(\alpha)$ and $\mathcal{L}_1(\alpha^{-1})$, albeit implicitly. It is at this place that several congruences from Section 2 for $\mathcal{L}_1$ and $\mathcal{L}_2$ can be brought into play, at the expense of the appearance of $\mathcal{L}_2(1-\alpha)$ and $\mathcal{L}_2(1-\alpha^{-1})$ as observed above.

Finally, Eq. (42) can be easily deduced from Eq. (41) using Eq. (19) with $n=p$. □

8. Numerical congruences

In this final section we illustrate how the special values of the finite polylogarithms investigated in Section 4 allow one to evaluate the polynomial congruences in Sections 6 and 7 at certain special

values of t, thus producing explicit numerical congruences, some of which were proved or conjectured in the literature.

For a given algebraic number $t \neq 0$, let α and α^{-1} be the two complex roots of the polynomial $x^2 - (2-t)x + 1$, whence $t = 2 - \alpha - \alpha^{-1}$. Then for $k \geqslant 0$ we have

$$u_k(2-t) = \begin{cases} \frac{\alpha^k - \alpha^{-k}}{\alpha - \alpha^{-1}} & \text{if } t \neq 4, \\ (-1)^k k & \text{if } t = 4, \end{cases} \quad \text{and} \quad v_k(2-t) = \alpha^k + \alpha^{-k}.$$

Consequently, for $d \geqslant 1$ we have

$$\sum_{k=1}^{p-1} \frac{u_k(2-t)}{k^d} = \begin{cases} \frac{\mathcal{L}_d(\alpha) - \mathcal{L}_d(\alpha^{-1})}{\alpha - \alpha^{-1}} & \text{if } t \neq 4, \\ \mathcal{L}_{d-1}(-1) & \text{if } t = 4, \end{cases} \quad \text{and} \quad \sum_{k=1}^{p-1} \frac{v_k(2-t)}{k^d} = \mathcal{L}_d(\alpha) + \mathcal{L}_d\big(\alpha^{-1}\big).$$

Using the special values of $\mathcal{L}_d(x)$ established in Section 3, Theorem 6.1 allows one to compute the explicit values of the sums in Eq. (2) (modulo p^3 or p as stated), for $d = 1, 2$ and various values of t. Theorem 5.3 then allows one to obtain analogous formulas for the case $d = 0$.

Values of t for which we have quoted or proved congruences for the corresponding $\mathcal{L}_d(\alpha)$ in Section 4 are the following, grouped together according to G-orbits of α:

$$4; \quad 1; \quad -1/2; \quad 2,\ (1 \pm i)/2; \quad 3,\ (1 \pm i\sqrt{3})/3; \quad -1,\ 2 \pm \sqrt{5} = \pm\phi^3.$$

To illustrate the kind of congruences that one obtains, we give full details of the case $t = -1$, where $\alpha = \phi_+^2$ and $\alpha^{-1} = \phi_-^2$. In this case $u_n = F_{2n}$ and $v_n = L_{2n}$, where F_k and L_k are respectively the k-th Fibonacci number and the k-th Lucas number. The evaluations modulo p of $\mathcal{L}_2(\phi_\pm^2)$ and $\mathcal{L}_3(\phi_\pm^2)$ which we obtained in Theorem 4.4 yield the following list of congruences. For comparison, to the right of each congruence we give the sum of the corresponding infinite series, which can be computed by using Eq. (1) and its derivatives at $z = i$. For reasons of space we omit the moduli from the congruences and specify them in the text.

For any prime $p > 5$, Eqs. (29), (30) and (26) yield the following three congruences modulo p:

$$p \sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}(2)}{k\binom{2k}{k}} \equiv \frac{1}{5}\left(\frac{p}{5}\right) q_L^2, \qquad \sum_{k=1}^{\infty} \frac{(-1)^k H_{k-1}(2)}{k\binom{2k}{k}} = \frac{4\sqrt{5}}{15} \log^3(\phi_+),$$

$$p \sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}(2)}{k^2\binom{2k}{k}} \equiv \frac{4}{15}\left(\frac{1}{2} q_L^3 + B_{p-3}\right), \qquad \sum_{k=1}^{\infty} \frac{(-1)^k H_{k-1}(2)}{k^2\binom{2k}{k}} = \frac{2}{3} \log^4(\phi_+),$$

$$p \sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}(2)}{\binom{2k}{k}} \equiv \frac{1}{5} q_L + \frac{2}{25}\left(\frac{p}{5}\right) q_L^2,$$

$$\sum_{k=1}^{\infty} \frac{(-1)^k H_{k-1}(2)}{\binom{2k}{k}} = \frac{2}{5} \log^2(\phi_+) + \frac{8\sqrt{5}}{75} \log^3(\phi_+).$$

Eqs. (27), (28) and (25) yield the following three congruences modulo p^3:

$$p \sum_{k=1}^{p-1} \frac{(-1)^k}{k\binom{2k}{k}} \equiv \frac{1 - L_p F_p}{2} + \frac{p^2}{5}\left(\frac{p}{5}\right) q_L^2, \qquad \sum_{k=1}^{\infty} \frac{(-1)^k}{k\binom{2k}{k}} = -\frac{2\sqrt{5}\log(\phi_+)}{5},$$

$$p\sum_{k=1}^{p-1}\frac{(-1)^k}{k^2\binom{2k}{k}}\equiv\frac{1-L_p^2}{2p}+\frac{4p^2}{15}\left(\frac{1}{2}q_L^3+B_{p-3}\right),\qquad \sum_{k=1}^{\infty}\frac{(-1)^k}{k^2\binom{2k}{k}}=-2\log^2(\phi_+),$$

$$p\sum_{k=1}^{p-1}\frac{(-1)^k}{\binom{2k}{k}}\equiv\frac{p-L_pF_p}{5}+\frac{2p^2}{25}\left(\frac{p}{5}\right)q_L^2,\qquad \sum_{k=1}^{\infty}\frac{(-1)^k}{\binom{2k}{k}}=-\frac{1}{5}-\frac{4\sqrt{5}}{25}\log(\phi_+).$$

We refrain from listing all of the congruences produced by our results for the remaining values of t listed earlier, but we point out that, to our knowledge, three of them were already known, and several were conjectured. The known ones were proved by Z.W. Sun in [23, Theorems 1.2 and 1.3], namely, [23, Eq. (1.6)] follows from our Eq. (30) with $t=2$, while [23, Eqs. (1.12) and (1.13)] follow from our Eqs. (30) and (37) with $t=4$. Furthermore, our congruences confirm some of the conjectures stated by Z.W. Sun in [21, A31], for $p>3$:

$$p\sum_{k=1}^{p-1}\frac{2^k}{k\binom{2k}{k}}\equiv\left(\frac{-1}{p}\right)-1-pq_p(2)+p^2E_{p-3}\pmod{p^3},$$

$$p\sum_{k=1}^{p-1}\frac{2^k}{k^2\binom{2k}{k}}\equiv-q_p(2)+\frac{p^2}{16}B_{p-3}\pmod{p^3},$$

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

Some congruences for the case $d=3$ can be obtained from Theorem 6.2, such as the following, for $p>3$:

$$p\sum_{k=1}^{p-1}\frac{4^k}{k^3\binom{2k}{k}}\equiv-4q_p(2)^2+p\left(\frac{4}{3}q_p(2)^3-\frac{1}{6}B_{p-3}\right)\pmod{p^2}.$$

In this case, values of t different from 4 are not as easy to deal with. One further integration using Lemma 5.1 allows one to obtain congruences with $d=4$ as well. Although we have not stated a corresponding result analogous to Theorem 6.2, we mention that one can derive the congruence, for $p>3$,

$$p\sum_{k=1}^{p-1}\frac{4^k}{k^4\binom{2k}{k}}\equiv-\frac{4}{3}\left(2q_p(2)^3+B_{p-3}\right)\pmod{p}.$$

Together with the special values of the finite dilogarithm computed in Section 4, Eq. (40) of Theorem 7.1 allows us to evaluate the sum $\sum_{k=0}^{p-1}\binom{2k}{k}t^{-k}\pmod{p^3}$ for the values of t mentioned earlier. Aside from the case $t=4$, which is trivial here because of the identity $\sum_{k=0}^{n}\binom{2k}{k}4^{-k}=(2n+1)\binom{2n}{n}4^{-n}$, two more of these evaluations were already known: the case $t=-1$ is [14, Theorem 1.3], and the case $t=2$ is [24, Theorem 1.1]. Our new contributions due to Eq. (40), for $p>3$, are

$$\sum_{k=0}^{p-1}\binom{2k}{k}\equiv\left(\frac{p}{3}\right)-\frac{p^2}{3}B_{p-2}(1/3)\pmod{p^3},$$

$$\sum_{k=0}^{p-1} \frac{\binom{2k}{k}}{3^k} \equiv \left(\frac{p}{3}\right) - \frac{2p^2}{9} B_{p-2}(1/3) \pmod{p^3},$$

$$\sum_{k=1}^{p-1} (-2)^k \binom{2k}{k} \equiv -\frac{4p}{3} q_p(2) \pmod{p^3}.$$

In a similar way, specializing Eqs. (41) and (42) produces several numerical congruences. Among those we mention

$$\sum_{k=1}^{p-1} \frac{(-1)^k}{k} \binom{2k}{k} \equiv -2q_L - pq_L^2 \pmod{p^2},$$

$$\sum_{k=1}^{p-1} \frac{\binom{2k}{k}}{k^2} \equiv \frac{1}{2}\left(\frac{p}{3}\right) B_{p-2}\left(\frac{1}{3}\right) \pmod{p},$$

which hold for any prime $p > 3$.

Even the irrational values of t in our list give rise to nice congruences with rational terms after combining the algebraic conjugates together. As an example, because $t = 2 \mp \sqrt{5} = \phi_{\mp}^3$ corresponds to $\alpha = \pm\phi_+$, and because $2\phi_{\pm}^n = L_n \pm \sqrt{5}F_n$, Eqs. (41) and (42) yield, for $p > 5$,

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{(-1)^k F_{3k-(\frac{p}{5})}}{k} \equiv \frac{1}{5} pq_L^2 \pmod{p^2},$$

$$\sum_{k=1}^{p-1} \binom{2k}{k} \frac{(-1)^k L_{3k-(\frac{p}{5})}}{k^2} \equiv 0 \pmod{p}.$$

Supplementary material

The online version of this article contains additional supplementary material. Please visit http://dx.doi.org/10.1016/j.jnt.2012.05.036.

References

[1] B.C. Berndt, Ramanujan's Notebooks, Part I, Springer-Verlag, New York, 1998.
[2] J.M. Borwein, D.J. Broadhurst, J. Kamnitzer, Central binomial sums, multiple Clausen values, and zeta values, Experiment. Math. 10 (2001) 25–34.
[3] J.M. Borwein, M. Chamberland, Integer powers of arcsin, Int. J. Math. Math. Sci. 2007 (2007), http://dx.doi.org/10.1155/2007/19381, Art. ID 19381, 10 pages.
[4] W. Chu, D. Zheng, Infinite series with harmonic numbers and central binomial coefficients, Int. J. Number Theory 5 (2009) 429–448.
[5] K. Dilcher, L. Skula, The cube of the Fermat quotient, Integers 6 (2006), #A24.
[6] P. Elbaz-Vincent, H. Gangl, On poly(ana)logs, I, Compos. Math. 130 (2002) 161–210.
[7] A. Granville, The square of the Fermat quotient, Integers 4 (2004), #A22.
[8] D.R. Heath-Brown, Heilbronn's exponential sums and transcendence theory, in: A Panorama of Number Theory or The View from Baker's Garden, Zürich, 1999, Cambridge Univ. Press, Cambridge, 2002.
[9] L. Lewin, Polylogarithms and Associated Functions, North-Holland, New York, 1981.
[10] L. Lewin, Structural Properties of Polylogarithms, Math. Surveys Monogr., vol. 37, American Mathematical Society, Providence, 1991.
[11] S. Mattarei, Artin–Hasse exponentials of derivations, J. Algebra 294 (2005) 1–18.
[12] S. Mattarei, R. Tauraso, Congruences of multiple sums involving sequences invariant under the binomial transform, J. Integer Seq. 13 (2010), 10.5.1.
[13] M. Mirimanoff, L'équation indéterminée $x^l + y^l + z^l = 0$ et le critérium de Kummer, J. Reine Angew. Math. 128 (1904) 45–68.

[14] H. Pan, Z.W. Sun, Proof of three conjectures on congruences, preprint, arXiv:1010.2489, 2010.
[15] Kh. Hessami Pilehrood, T. Hessami Pilehrood, Congruences arising from Apéry-type series for zeta values, Adv. in Appl. Math. (2012), http://dx.doi.org/10.1016/j.aam.2012.05.003, preprint arXiv:1108.1893v2.
[16] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag, New York, Heidelberg, 1979.
[17] H. Strade, Simple Lie Algebras over Fields of Positive Characteristic, I. Structure Theory, de Gruyter, Berlin, 2004.
[18] Z.H. Sun, Congruences concerning Bernoulli numbers and Bernoulli polynomials, Discrete Appl. Math. 105 (2000) 193–223.
[19] Z.H. Sun, Congruences involving Bernoulli polynomials, Discrete Math. 308 (2008) 71–112.
[20] Z.H. Sun, Congruences involving Bernoulli and Euler numbers, J. Number Theory 128 (2008) 280–312.
[21] Z.W. Sun, Open conjectures on congruences, preprint, arXiv:0911.5665v49, 2010.
[22] Z.W. Sun, Binomial coefficients, Catalan numbers and Lucas quotients, Sci. China Math. 53 (2010) 2473–2488.
[23] Z.W. Sun, A new series for π^3 and related congruences, preprint, arXiv:1009.5375v6, 2010.
[24] Z.W. Sun, Supercongruences and Euler numbers, Sci. China Math. 54 (2011) 2509–2535.
[25] Z.W. Sun, R. Tauraso, New congruences for central binomial coefficients, Adv. Math. 45 (2010) 125–148.
[26] R. Tauraso, More congruences for central binomial coefficients, J. Number Theory 130 (2010) 2639–2649.
[27] R. Tauraso, J. Zhao, Congruences of alternating multiple harmonic sums, J. Comb. Number Theory 2 (2010) 129–159.
[28] A. van der Poorten, A proof that Euler missed... Apéry's proof of the irrationality of $\zeta(3)$. An informal report, Math. Intelligencer 1 (4) (1978/1979) 195–203.
[29] R. Wituła, D. Słota, Finite sums connected with the inverses of central binomial numbers and Catalan numbers, Asian-Eur. J. Math. 1 (2008) 439–448.
[30] J. Zhao, Bernoulli numbers, Wolstenholme's theorem, and p^5 variations of Lucas' theorem, J. Number Theory 123 (2007) 18–26.
[31] X. Zhou, T. Cai, A generalization of a curious congruence on harmonic sums, Proc. Amer. Math. Soc. 135 (2007) 1329–1333.