Partial Lucas-type congruences

(Dedicated to George Andrews and Bruce Berndt for their 85$^{\text{th}}$ birthdays)

Armin Straub*
Department of Mathematics and Statistics
University of South Alabama

November 2, 2025

Abstract

In their study of a binomial sum related to Wolstenholme's theorem, Chamberland and Dilcher prove that the corresponding sequence modulo primes p satisfies congruences that are analogous to Lucas' theorem for the binomial coefficients with the notable twist that there is a restriction on the p-adic digits. We prove a general result that shows that similar partial Lucas congruences are satisfied by all sequences representable as the constant terms of the powers of a multivariate Laurent polynomial.

1 Introduction

Chamberland and Dilcher [CD06] study divisibility properties of the sequences $(u^{\varepsilon}_{a,b}(n))_{n\geq 0}$ defined by the binomial sums

$$u^{\varepsilon}_{a,b}(n) = \sum_{k=0}^{n} (-1)^{\varepsilon k} \binom{n}{k}^a \binom{2n}{k}^b \tag{1}$$

and connect these sums to Wolstenholme's theorem. In the follow-up study [CD09], they further investigate the special case $(\varepsilon, a, b) = (1, 1, 1)$

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

which is sequence `A234839` in the OEIS [OEI25]. One of the interesting arithmetic properties that Chamberland and Dilcher [CD09] prove is the following set of congruences which, as we recall below, can be viewed as partial Lucas congruences.

* *Email:* straub@southalabama.edu

Theorem 1.1 ([CD09, Theorem 2.2]). *Let $p \geq 3$ be a prime. Then*

$$u(pn+k) \equiv u(n)u(k) \pmod{p}$$

for all integers $n, k \geq 0$ with $k \leq (p-1)/2$.

Let p, here and throughout, denote a prime, while n and k are used to denote non-negative integers. It follows immediately, as observed in [CD09, Corollary 2.1], that, if $n = n_0 + n_1 p + \cdots + n_r p^r$ is the p-adic expansion of n, then

$$u(n) \equiv u(n_0)u(n_1)\cdots u(n_r) \pmod{p}, \tag{3}$$

provided that $0 \leq n_j < p/2$ for all $j = 0, 1, \ldots, r$. These congruences are reminiscent of the classical congruences

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_r}{k_r} \pmod{p} \tag{4}$$

for the binomial coefficients due to Lucas [Luc78] where $n = n_0 + n_1 p + \cdots + n_r p^r$ and $k = k_0 + k_1 p + \cdots + k_r p^r$ with $0 \leq n_j, k_j < p$.

For the sequence $(u(n))_{n\geq 0}$ from (2), the congruences (3) are restricted to digits n_j less than $p/2$. On the other hand, Gessel showed [Ges82, Theorem 1] that the Apéry numbers

$$A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \tag{5}$$

in place of $u(n)$ satisfy the congruences (3) for all digits $0 \leq n_j < p$ (see also Example 2.4). Accordingly, we say that the Apéry numbers satisfy *Lucas congruences* modulo all primes, and the same has since been shown to be true for many other (families of) sequences [McI92], [Gra97], [SvS15], [RY15], [MS16], [Del18], [ABD19], [Gor21], [HS22]. A historical survey of Lucas congruences can be found in [Me4]. On the other hand, the sequence $(u(n))_{n\geq 0}$ satisfies the Lucas congruences only partially.

Chamberland and Dilcher [CD09] proved Theorem 1.1 directly from the binomial sum (2) using the Lucas congruences (4) for the binomial coefficients. We show that Theorem 1.1, as well as similar results, can be uniformly proved for a large class of sequences representable as *constant terms*. Here, we say that a sequence $(c(n))_{n\geq 0}$ is a constant term if it can be expressed as

$$c(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$$

for Laurent polynomials $P(\boldsymbol{x}), Q(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ in several variables $\boldsymbol{x} = (x_1, x_2, \ldots, x_d)$ with integer coefficients. Throughout, we use the notation $\mathrm{ct}[F(\boldsymbol{x})]$ for the constant term of a Laurent polynomial $F(\boldsymbol{x})$ in the variables $\boldsymbol{x}$. As further detailed in Section 2, we denote with $\mathrm{Newt}(P)$ the Newton polytope of P. Our main result shows that all constant term sequences with $Q = 1$ satisfy partial Lucas congruences.

Theorem 1.2. *Let $P(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ and choose $M \geq 1$ large enough so that $\frac{1}{M}\operatorname{Newt}(P)$ contains no integral (relative) interior point besides the origin. Then, for all primes p, the sequence defined by $A(n) = \operatorname{ct}[P(\boldsymbol{x})^n]$ satisfies*

$$A(pn+k) \equiv A(n)A(k) \pmod{p}$$

for all integers $n, k \geq 0$ with $k < \frac{p}{M}$.

We note that the special case $M = 1$ of Theorem 1.2, which proves that certain constant terms satisfy the (full) Lucas congruences modulo all primes, also follows from a result of Samol and van Straten [SvS15, Theorem 4.3] (see also [MV16] and [HS22]). We prove Theorem 1.2 in Section 2 and speculate about a potential converse in Question 2.6. As a first example, we observe here that it implies Theorem 1.1 as a special case.

Example 1.3. We will show below that the sequence $(u(n))_{n\geq 0}$ defined in (2) has the constant term representation

$$u(n) = \operatorname{ct}\left[\left((1+x)\left(x-\frac{1}{x}\right)\right)^n\right]. \tag{6}$$

Clearly, the Newton polytope of $P(x) = (1+x)\left(x-\frac{1}{x}\right) = x^2+x-1-\frac{1}{x}$ is the interval $\operatorname{Newt}(P) = [-1,2]$. In particular, $\frac{1}{2}\operatorname{Newt}(P) = \left[-\frac{1}{2},1\right]$ contains no integral interior point besides 0. Therefore, Theorem 1.2 applies with $M = 2$ to show that Theorem 1.1 indeed holds for all primes (note that Theorem 1.1 holds rather vacuously for $p = 2$).

In principle, once found, a constant term representation such as (6) can be algorithmically proven using creative telescoping [Kou09] (see, for instance, [Gor21] for worked-out examples). In general, however, it is a difficult problem to find constant term representations (or even to decide whether such a representation exists; see [BSY23]). Yet, certain binomial sums can be systematically translated into constant term representations. This is explained by Rowland and Zeilberger in [RZ14] who attribute the approach to Egorychev. In the present case we readily obtain

$$\begin{aligned} u(n) &= \sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{2n}{k} \\ &= \operatorname{ct}\left[\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{(1+x)^{2n}}{x^k}\right] \\ &= \operatorname{ct}\left[(1+x)^{2n}\left(1-\frac{1}{x}\right)^n\right], \end{aligned}$$

which is equivalent to the claimed representation.

We illustrate the versatility of Theorem 1.2 by showing that Theorem 1.1 for the sequence defined by $u(n) = u^1_{1,1}(n)$ actually continues to hold for the more general sequence $(u^{\varepsilon}_{a,b}(n))_{n\geq 0}$ defined in (1).

Corollary 1.4. *For any prime p and any integers ε, $a \geq 1$, $b \geq 0$ we have*

$$u^{\varepsilon}_{a,b}(pn+k) \equiv u^{\varepsilon}_{a,b}(n)u^{\varepsilon}_{a,b}(k) \pmod{p}$$

for all integers $n, k \geq 0$ with $k < p/2$.

Proof. We can readily express $u^{\varepsilon}_{a,b}(n)$ as a constant term as follows:

$$\begin{aligned} u^{\varepsilon}_{a,b}(n) &= \sum_{k=0}^{n}(-1)^{\varepsilon k}\binom{n}{k}^a\binom{2n}{k}^b \\ &= \operatorname{ct}\left[\sum_{k=0}^{n}(-1)^{\varepsilon k}\binom{n}{k}\prod_{i=1}^{a-1}\frac{(1+x_i)^n}{x_i^k}\prod_{j=a}^{a+b-1}\frac{(1+x_j)^{2n}}{x_j^k}\right] = \operatorname{ct}[P(\boldsymbol{x})^n] \end{aligned} \tag{7}$$

with the Laurent polynomial

$$P(\boldsymbol{x}) = \left(1+\frac{(-1)^{\varepsilon}}{x_1\cdots x_{a+b-1}}\right)\prod_{i=1}^{a-1}(1+x_i)\prod_{j=a}^{a+b-1}(1+x_j)^2.$$

Note that $\operatorname{Newt}(P) \subseteq [-1,2]^{a+b-1}$ so that we can apply Theorem 1.2 with $M=2$ to arrive at the claimed congruences. □

If desired, further generalizations beyond the sequence $(u^{\varepsilon}_{a,b}(n))_{n\geq 0}$ can be given along the same lines (for instance, one can replace $(-1)^{\varepsilon}$ by any integer r and one can insert additional powers of suitable binomial coefficients such as $\binom{n+k}{k}$ into the summation).

2 Partial Lucas congruences

When working with several variables $\boldsymbol{x} = (x_1, x_2, \ldots, x_d)$, we use common shorthand notation to write, for instance, $\boldsymbol{x}^{\boldsymbol{v}} = x_1^{v_1}x_2^{v_2}\cdots x_d^{v_d}$ where the exponents are specified in the vector $\boldsymbol{v} = (v_1, v_2, \ldots, v_d)$. Given a Laurent polynomial

$$P(\boldsymbol{x}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^d} c_{\boldsymbol{v}}\boldsymbol{x}^{\boldsymbol{v}} \in R[\boldsymbol{x}^{\pm 1}]$$

over some ring R of characteristic 0, its support is

$$\operatorname{supp}(P) = \left\{\boldsymbol{v}\in\mathbb{Z}^d \,:\, c_{\boldsymbol{v}} \neq 0\right\}.$$

For subsets S, T of a vector space and scalars λ, we use the typical notations $\lambda S = \{\lambda\boldsymbol{v} \,:\, \boldsymbol{v}\in S\}$ and $S+T = \{\boldsymbol{v}+\boldsymbol{w} \,:\, \boldsymbol{v}\in S, \boldsymbol{w}\in T\}$, the latter being the Minkowski sum. For instance, we note that $\operatorname{supp}(PQ) \subseteq \operatorname{supp}(P) + \operatorname{supp}(Q)$ for Laurent polynomials P, Q.

Some care has to be applied since $2S \subseteq S+S$ while, in general, $2S \neq S+S$. Such issues disappear if we work with convex sets. Indeed, for all convex sets S we do have $2S = S+S$ (to see this, take $\boldsymbol{v}, \boldsymbol{w} \in S$ and note that $\boldsymbol{v}+\boldsymbol{w} = 2\left(\frac{1}{2}\boldsymbol{v}+\frac{1}{2}\boldsymbol{w}\right) \in 2S$ because convexity of S implies that $\frac{1}{2}\boldsymbol{v}+\frac{1}{2}\boldsymbol{w} \in S$). For further background, we refer to [Sch93]. The Newton polytope of P, denoted as $\mathrm{Newt}(P)$, is the convex hull of $\mathrm{supp}(P)$. In other words,

$$\mathrm{Newt}(P) = \left\{ \sum_{\boldsymbol{v}\in\mathrm{supp}(P)} \lambda_{\boldsymbol{v}}\boldsymbol{v} \,:\, \lambda_{\boldsymbol{v}} \geq 0, \sum_{\boldsymbol{v}\in\mathrm{supp}(P)} \lambda_{\boldsymbol{v}} = 1 \right\}. \tag{8}$$

It is a well-known basic property of Newton polytopes that

$$\mathrm{Newt}(PQ) = \mathrm{Newt}(P) + \mathrm{Newt}(Q) \tag{9}$$

for all Laurent polynomials P, Q.

To make the statement of Theorem 1.2 more transparent, we make the simple observation that, when considering nontrivial sequences defined by $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$, the Newton polytope always contains the origin.

Proposition 2.1. *Let $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ for $P(\boldsymbol{x}) \in \mathbb{C}[\boldsymbol{x}^{\pm 1}]$. If $A(n) \neq 0$ for some $n \geq 1$, then $\mathrm{Newt}(P)$ contains the origin.*

Proof. If $A(n) \neq 0$ for $n \geq 1$ then, by definition, the origin is in the support of $P(\boldsymbol{x})^n$ so that, in particular, $\mathbf{0} \in \mathrm{Newt}(P^n)$. Since Newton polytopes are convex by definition, it follows from (9) that

$$\mathrm{Newt}(P^n) = n\,\mathrm{Newt}(P).$$

Thus, $\mathbf{0} \in n\,\mathrm{Newt}(P)$ and, since $n \neq 0$, we also have $\mathbf{0} \in \mathrm{Newt}(P)$. □

Let $\gamma > 0$. If $\mathbf{0} \in \mathrm{Newt}(P)$ then, corresponding to (8), the (relative) interior points of $\gamma\,\mathrm{Newt}(P)$ are those that can be expressed as $\sum_{\boldsymbol{v}\in\mathrm{supp}(P)} \lambda_{\boldsymbol{v}}\boldsymbol{v}$ with $\lambda_{\boldsymbol{v}} \geq 0$ and $\sum_{\boldsymbol{v}\in\mathrm{supp}(P)} \lambda_{\boldsymbol{v}} < \gamma$.

We are now in a position to prove Theorem 1.2 which we restate as Theorem 2.2 in a slightly more general form, writing $\mathbb{Z}_p$ for the ring of p-adic integers. Our proof is an extension of the argument in [HS22] where the special case $M = 1$ is proved.

Theorem 2.2. *Let $P(\boldsymbol{x}) \in \mathbb{Z}_p[\boldsymbol{x}^{\pm 1}]$ and choose $M \geq 1$ so that $\frac{1}{M}\,\mathrm{Newt}(P)$ contains no integral (relative) interior point besides the origin. Then the sequence defined by $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ satisfies*

$$A(pn+k) \equiv A(n)A(k) \pmod{p} \tag{10}$$

for all integers $n, k \geq 0$ with $k < \frac{p}{M}$.

Proof. Let us denote with Λ_p the Cartier operator

$$\Lambda_p\left[\sum_{\boldsymbol{k}\in\mathbb{Z}^d} a_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}\right] = \sum_{\boldsymbol{k}\in\mathbb{Z}^d} a_{p\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}.$$

Let $n, k \geq 0$. Using that $P(\boldsymbol{x})^{pn} \equiv P(\boldsymbol{x}^p)^n$ modulo p and proceeding as in [HS22] and [BSY23], we have

$$\begin{aligned} A(pn+k) &= \operatorname{ct}[P(\boldsymbol{x})^{pn}P(\boldsymbol{x})^k] \\ &\equiv \operatorname{ct}[P(\boldsymbol{x}^p)^n P(\boldsymbol{x})^k] \pmod{p} \\ &= \operatorname{ct}[P(\boldsymbol{x})^n \Lambda_p[P(\boldsymbol{x})^k]]. \end{aligned} \tag{11}$$

Let $c\boldsymbol{x}^{\boldsymbol{v}}$, with $c \neq 0$, be a term of $\Lambda_p[P(\boldsymbol{x})^k]$. This means that $c\boldsymbol{x}^{p\boldsymbol{v}}$ is a term of $P(\boldsymbol{x})^k$ so that, in particular,

$$p\boldsymbol{v} = \lambda_1\boldsymbol{v}_1 + \lambda_2\boldsymbol{v}_2 + \cdots + \lambda_t\boldsymbol{v}_t$$

where $\boldsymbol{v}_i \in \operatorname{supp}(P) \subseteq \operatorname{Newt}(P)$, $\lambda_i \in \mathbb{Z}_{\geq 0}$ and $\lambda_1 + \lambda_2 + \cdots + \lambda_t = k$. Accordingly,

$$\boldsymbol{v} = \mu_1\boldsymbol{v}_1 + \mu_2\boldsymbol{v}_2 + \cdots + \mu_t\boldsymbol{v}_t, \quad \mu_i = \frac{\lambda_i}{p}, \tag{12}$$

where $\mu_i \geq 0$ and $\mu_1 + \cdots + \mu_t = k/p < \frac{1}{M}$. By Proposition 2.1, we may assume that $\mathbf{0} \in \operatorname{Newt}(P)$ since the congruences (10) are trivially true otherwise. We then observe that, since $\mathbf{0} \in \operatorname{Newt}(P)$, the (relative) interior points of $\frac{1}{M}\operatorname{Newt}(P)$ are those that can be expressed as $\sum_{\boldsymbol{v}\in\operatorname{supp}(P)} \lambda_{\boldsymbol{v}}\boldsymbol{v}$ with $\lambda_{\boldsymbol{v}} \geq 0$ and $\sum_{\boldsymbol{v}\in\operatorname{supp}(P)} \lambda_{\boldsymbol{v}} < \frac{1}{M}$ (compare with (8)). Accordingly, the point $\boldsymbol{v}$ in (12) is an integral interior point of $\frac{1}{M}\operatorname{Newt}(P)$. Hence $\boldsymbol{v} = \mathbf{0}$ since, by assumption, there are no other integral interior points. We conclude that

$$\Lambda_p[P(\boldsymbol{x})^k] = \operatorname{ct}[P(\boldsymbol{x})^k]$$

which, together with (11), implies that

$$A(pn+k) \equiv \operatorname{ct}[P(\boldsymbol{x})^n \operatorname{ct}[P(\boldsymbol{x})^k]] = \operatorname{ct}[P(\boldsymbol{x})^n]\operatorname{ct}[P(\boldsymbol{x})^k] = A(n)A(k) \pmod{p},$$

thus showing (10). □

We record the following simple special case of Theorem 2.2 that is particularly convenient to apply. However, as illustrated in Examples 2.4 and 2.7, it does not capture the full strength of Theorem 2.2. Here, we denote with $\deg(P)$ the largest exponent to which any variable x_i or its inverse x_i^{-1} appears in the Laurent polynomial $P(\boldsymbol{x})$.

Corollary 2.3. *Let $P(\boldsymbol{x}) \in \mathbb{Z}_p[\boldsymbol{x}^{\pm 1}]$. Then the sequence defined by $A(n) = \operatorname{ct}[P(\boldsymbol{x})^n]$ satisfies*

$$A(pn+k) \equiv A(n)A(k) \pmod{p}$$

for integers $n, k \geq 0$ with $k < \frac{p}{\deg(P)}$.

Proof. This follows directly from Theorem 2.2 with $M = \deg(P)$. Alternatively, this can be concluded from [BSY23, Lemma 3.1] with $r = 1$ and $Q = 1$. □

Example 2.4. The Apéry numbers $A(n)$, defined in (5), have the constant term representation [Str14, Remark 1.4]

$$A(n) = \mathrm{ct}[P(\boldsymbol{x})^n], \quad P(\boldsymbol{x}) = \frac{(x+y)(z+1)(x+y+z)(y+z+1)}{xyz}.$$

Since the Newton polytope of $P(\boldsymbol{x})$ contains no integral interior point besides the origin, it immediately follows from Theorem 2.2 (with $M = 1$) that the Apéry numbers $A(n)$ satisfy the Lucas congruences for all primes, as proved directly from the binomial sum (5) by Gessel [Ges82, Theorem 1]. On the other hand, note that Corollary 2.3 only provides weaker partial Lucas congruences because $\deg(P) = 2$.

Remark 2.5. Suppose that $P, Q \in \mathbb{Z}_p[\boldsymbol{x}^{\pm 1}]$. We briefly indicate that Theorem 2.2 indirectly also applies to constant terms of the form $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$ when $Q \neq 1$. In that case it follows, for instance, from [BSY23, Lemma 3.1] with $r = 1$ that

$$A(pn + k) \equiv A(k)B(n) \pmod{p} \tag{13}$$

where $B(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ provided that $p > \deg(P^k Q)$. The condition on p is satisfied if $p > k\deg(P) + \deg(Q)$ or, equivalently, $k < \frac{p-\deg(Q)}{\deg(P)}$. In light of (13), by applying Theorem 2.2 to the constant term $B(n)$, we can determine the values of $A(n)$ modulo p provided that the p-adic digits of n are suitably restricted (to satisfy the conditions needed for (13) as well the subsequent applications of Theorem 2.2).

It is natural to wonder about a possible converse statement of Theorem 2.2. For instance, if a constant term sequence $(A(n))_{n\geq 0}$ satisfies partial Lucas congruences, does there always exist a, potentially alternative, representation $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ such that these congruences can be concluded from Theorem 2.2? In other words:

Question 2.6. *Suppose that $A(n) = \mathrm{ct}[P_0(\boldsymbol{x})^n Q_0(\boldsymbol{x})]$ with $P_0, Q_0 \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ is a constant term that satisfies $A(0) = 1$ as well the Lucas congruences (10) for integers $n, k \geq 0$ with $k < \frac{p}{M}$. Does $A(n)$ necessarily have a representation $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ for some $P(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ with $\frac{1}{M}\mathrm{Newt}(P)$ containing no integral interior point besides the origin? If not, is this true under an additional natural condition?*

We make two comments on the statement of this question before illustrating the question and its implications in two special instances. First, we note that the condition $A(0) = 1$ should be seen as part of satisfying the Lucas congruences: indeed, the Lucas congruences in the alternative form (3) naturally imply $A(0) = 1$ if we apply them for $n = 0$ with an empty p-adic expansion so that the right-hand side of (3) is the empty product with

value 1. Moreover, the condition $A(0) = 1$ is needed to avoid the case of the zero sequence which can be represented as a constant term with $P = 1$ and $Q = x$ and which trivially satisfies the congruences (10) (but, clearly, cannot have a representation of the form $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$).

Second, we observe that there is no loss of generality in reducing to the case $Q_0(\boldsymbol{x}) = 1$ in Question 2.6. Indeed, if $A(n)$ satisfies the Lucas congruences (10) for integers $n, k \geq 0$ with $k < \frac{p}{M}$ then, in particular,

$$A(pn) \equiv A(n) \pmod{p}.$$

In [BSY23, Proposition 5.1] it is shown that, for constant terms, these congruences imply, for large enough p, the stronger congruences

$$A(p^r n) \equiv A(p^{r-1} n) \pmod{p^r} \tag{14}$$

(known in the literature as Gauss congruences) and that, in fact, $A(n) = A(0)\,\mathrm{ct}[P_0(\boldsymbol{x})^n] = \mathrm{ct}[P_0(\boldsymbol{x})^n]$ (that is, $Q_0(\boldsymbol{x})$ can be replaced by 1 in the constant term representation that we started with).

The following example illustrates Question 2.6 for a specific sequence. In that particular case, the answer to Question 2.6 is affirmative.

Example 2.7. Consider the generalized Delannoy sequence [OEI25, `A081798`]

$$C(n) = \sum_{k=0}^{n} \binom{n}{k} \binom{n+k}{k} \binom{n+2k}{k},$$

which starts with the values $1, 7, 115, 2371, 54091, \ldots$ and counts lattice walks from the origin to (n, n, n) using steps $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ and $(1, 1, 1)$.

We can proceed as in Example 1.3 to express $C(n)$ as the constant term

$$C(n) = \mathrm{ct}\left[\sum_{k=0}^{n} \binom{n}{k} \frac{(1+x)^{n+k}}{x^k} \frac{(1+y)^{n+2k}}{y^k}\right] = \mathrm{ct}[P(x,y)^n]$$

with

$$P(x,y) = (1+x)(1+y)\left(1 + \frac{1+x}{x}\frac{(1+y)^2}{y}\right).$$

The Laurent polynomial P has support $\{-1, 0, 1\} \times \{-1, 0, 1, 2\}$. In particular, its Newton polytope is the rectangle $[-1, 1] \times [-1, 2]$ which has the interior integral points $(0, 0)$ and $(0, 1)$. Hence, Theorem 1.2 can be applied with $M = 2$ to deduce partial Lucas congruences.

However, it follows from a result of McIntosh [McI92, Theorem 6] that the sequence $(C(n))_{n\geq 0}$ satisfies the full Lucas congruences for all primes. We note that this can also be concluded from expressing $C(n)$ as the diagonal of the rational function $1/(1 - x - y -$

$z - xyz$), which naturally encodes the lattice walk count, and applying a general result of Rowland and Yassawi [RY15, Theorem 5.2]. It is therefore a natural special case of Question 2.6 to ask whether the sequence $(C(n))_{n\geq 0}$ has an alternative constant term representation such that Theorem 1.2 can be applied with $M = 1$ to deduce the full Lucas congruences. In this case, the answer is affirmative. Indeed, we can also write

$$C(n) = \sum_{k=0}^{n} \binom{n}{k}\binom{n+2k}{k,k,n} = \mathrm{ct}\left[\sum_{k=0}^{n} \binom{n}{k} \frac{(1+x+y)^{n+2k}}{x^k y^k}\right] = \mathrm{ct}[\tilde{P}(x,y)^n]$$

with

$$\tilde{P}(x,y) = (1+x+y)\left(1+\frac{(1+x+y)^2}{xy}\right).$$

The Newton polytope of $\tilde{P}$ is the triangle with vertices $(-1,-1)$, $(-1,2)$, $(2,-1)$. Its only interior integral point is $(0,0)$ and so Theorem 1.2 applies with $M = 1$ and we are able to conclude the full Lucas congruences.

Example 2.8. The following is a specific instance for which it would be of particular interest to know the answer to Question 2.6. Consider the constant term sequence $(A(n))_{n\geq 0}$ defined by $A(n) = \mathrm{ct}[P^n]$ with the symmetric Laurent polynomial

$$P = \frac{(zx+xy-yz-x-1)(xy+yz-zx-y-1)(yz+zx-xy-z-1)}{xyz}.$$

This representation was recently discovered by Gorodetsky [Gor21] through a clever computational search. Gorodetsky succeeded in finding such constant term representations for all known *sporadic* Apéry-like sequences, the present sequence $(A(n))_{n\geq 0}$ typically being labeled (η) in the literature [AvSZ11]. For all sporadic Apéry-like sequences besides (η), these constant term representations are such that the Newton polytope of the underlying Laurent polynomial only has the origin as an interior integral point, thus implying (as in Example 2.4 for the Apéry numbers) that the sequence satisfies the Lucas congruences. The Newton polytope of the above Laurent polynomial P, however, contains the lattice points $(1,0,0)$, $(1,1,0)$ and their permutations as interior points so that the Lucas congruences cannot be directly concluded (though Theorem 2.2 can be applied with $M = 2$ to imply Lucas congruences if the digits are less than $p/2$). Nevertheless, Malik and the author [MS16] had previously shown that all known sporadic Apéry-like sequences satisfy Lucas congruences (with the case (η) requiring an ad-hoc and technical argument). It is natural to wonder whether the sequence (η) has a, yet-to-be-discovered, constant term representation $A(n) = \mathrm{ct}[\tilde{P}(\boldsymbol{x})^n]$ such that the Newton polytope of $\tilde{P}$ only has the origin as an interior integral point. An affirmative answer to Question 2.6 would imply that such a representation exists. In any case, this example and its history underscore the difficulty in finding constant term representations for a given sequence. On the other hand, as pointed out in the introduction, constant term representations, once found, can be algorithmically proven (at least in principle) using, for instance, creative telescoping [Kou09].

3 More general congruences

In addition to establishing Theorem 1.1, the partial Lucas congruences for the sequence $(u(n))_{n\geq 0}$, Chamberland and Dilcher [CD09] further prove the following congruences, covering the p-adic digits that are excluded in the partial Lucas congruences.

Theorem 3.1 ([CD09, Corollary 2.2]). *Let*

$$w(n) = \sum_{k=0}^{n-1} (-1)^k \binom{2n-1}{k} \binom{n-1}{k}. \tag{15}$$

Then

$$u(pn+k) \equiv w(n+1)u(k) \pmod{p} \tag{16}$$

for all integers $n, k \geq 1$ with $(p+1)/2 \leq k < p$.

In [CD09], this result is obtained by working directly with the binomial sum (2) defining the numbers $u(n)$. In this section, we give an alternative proof of Theorem 3.1 using the constant term representation (6). This proof has the benefit of being natural in the sense that similar computations can be performed for other constant term sequences, though the present case offers some additional and nongeneric simplifications. In particular, our proof makes the relationship between the sequences $(u(n))_{n\geq 0}$ and $(w(n))_{n\geq 0}$ transparent from the point of view of constant terms (compare (6) and (19)). Further examples where similar congruences are explicitly worked out for a class of constant term sequences can be found in [HS22].

Proof. Recall from (6) that

$$u(n) = \mathrm{ct}[P(x)^n], \quad P(x) = (1+x)^2 \left(1 - \frac{1}{x}\right).$$

We therefore have, as in (11), that, modulo p,

$$\begin{aligned} u(pn+k) &= \mathrm{ct}[P(x)^{pn} P(x)^k] \\ &\equiv \mathrm{ct}[P(x^p)^n P(x)^k] \pmod{p} \\ &= \mathrm{ct}[P(x)^n \Lambda_p[P(x)^k]]. \end{aligned}$$

If $0 \leq k < p/2$, then $\Lambda_p[P(x)^k] = \mathrm{ct}[P(x)^k] = u(k)$ and we obtain the partial Lucas congruences $u(pn+k) \equiv u(n)u(k)$ that were obtained more generally in Theorem 2.2. Here, we assume that $(p+1)/2 \leq k < p$, in which case we find

$$\Lambda_p[P(x)^k] = \mathrm{ct}[P(x)^k] + x[x^p]P(x)^k, \tag{17}$$

where $[x^m]f(x)$ denotes the coefficient of x^m in the power series $f(x)$. Here, we used the fact that the largest exponent of x among all terms in $P(x)^k$ is $2k < 2p$ while the smallest exponent is $-k > -p$.

In general, we now need to investigate the numbers $c_p(k) = [x^p]P(x)^k$. In the present case, however, we have the remarkable simplification

$$[x^p]P(x)^k \equiv \mathrm{ct}[P(x)^k] \pmod{p} \tag{18}$$

for $(p+1)/2 \le k < p$, which we will prove below. Assuming for now the truth of (18) and combining it with (17), we obtain that

$$\Lambda_p[P(x)^k] \equiv (1+x)\,\mathrm{ct}[P(x)^k] = (1+x)u(k) \pmod{p}.$$

In particular, we conclude that

$$u(pn+k) \equiv \mathrm{ct}[P(x)^n \Lambda_p[P(x)^k]] \equiv \mathrm{ct}[P(x)^n(1+x)] \cdot u(k) = v(n)u(k) \pmod{p},$$

which proves generalized Lucas congruences involving the auxiliary sequence defined by

$$v(n) = \mathrm{ct}[P(x)^n(1+x)].$$

Indeed, this constant term sequence is precisely the sequence $(w(n+1))_{n\ge 0}$ introduced by Chamberland and Dilcher as the binomial sum (15). This can be seen from the following computation

$$\begin{aligned} w(n+1) &= \sum_{k=0}^{n} (-1)^k \binom{2n+1}{k}\binom{n}{k} \\ &= \mathrm{ct}\left[\sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{(1+x)^{2n+1}}{x^k}\right] \\ &= \mathrm{ct}\left[(1+x)^{2n+1}\left(1-\frac{1}{x}\right)^n\right] = \mathrm{ct}[P(x)^n(1+x)], \end{aligned} \tag{19}$$

which is along the same lines as the earlier derivation of (6).

It remains to show that (18) is true for $(p+1)/2 \le k < p$. Since $[x^p]P(x)^k = \mathrm{ct}[x^{-p}P(x)^k]$, the congruence (18) is equivalent to

$$\mathrm{ct}[(1-x^{-p})P(x)^k] \equiv 0 \pmod{p}. \tag{20}$$

Since $P(x) = (1+x)^2\left(1-\frac{1}{x}\right)$, we have

$$\mathrm{ct}[(1-x^{-p})P(x)^k] = \mathrm{ct}\left[\left(1-\frac{1}{x^p}\right)(1+x)^p(1+x)^{2k-p}\left(1-\frac{1}{x}\right)^k\right].$$

Using $(1+x)^p \equiv (1+x^p)$ modulo p and $(1-x^{-p})(1+x^p) = (x^p - x^{-p})$, we conclude

$$\operatorname{ct}[(1-x^{-p})P(x)^k] \equiv \operatorname{ct}\left[\left(x^p - \frac{1}{x^p}\right)(1+x)^{2k-p}\left(1-\frac{1}{x}\right)^k\right] \pmod{p}.$$

The right-hand side is now seen to be 0 because $(1+x)^{2k-p}$ is a polynomial (here, we use that $k \geq (p+1)/2$) in x of degree at most $2k-p < p$ while $(1-x^{-1})^k$ is a polynomial in x^{-1} of degree at most $k < p$ (and so the product does not have a term that is a multiple of either x^p or x^{-p}). This proves (20). □

4 Conclusions

We have shown that all sequences representable as the constant terms of the powers of a multivariate Laurent polynomial satisfy Lucas congruences modulo all primes with a restriction on the allowed digits. In a related but somewhat different direction, Rowland [Row22] considers the classical Lucas congruences (4) for the binomial coefficients and characterizes those digits (r, s) in base p such that the congruences

$$\binom{pn+r}{pk+s} \equiv \binom{n}{k}\binom{r}{s} \pmod{p^2}$$

hold for all integers $n, k \geq 0$. Rowland, Yassawi and Krattenthaler [RYK21] further consider the question of partial Lucas congruences modulo p^2 for the Apéry numbers (5). In general, such congruences modulo higher powers of p are more isolated than the general congruences in Theorem 1.2.

A motivation of the works of Chamberland and Dilcher [CD06, CD09] was the fact that the sequences $(u^{\varepsilon}_{a,b}(n))_{n\geq 0}$ defined in (1) are connected to Wolstenholme's theorem. Indeed, they show that

$$u^{\varepsilon}_{a,b}(p) \equiv 1 + (-1)^{\varepsilon}2^b \pmod{p^3}$$

for any prime $p \geq 5$, except when $(\varepsilon, a, b) = (0, 0, 1)$ or $(0, 1, 0)$. It remains an open problem to understand the composite numbers n satisfying this congruence as well. Andrews [And99] obtained a q-analog of Wolstenholme's congruences for the binomial coefficients. In this spirit, it could be of interest to develop a q-version of the present results.

The sequences $(u(n))_{n\geq 0}$ and $(u^{\varepsilon}_{a,b}(n))_{n\geq 0}$ studied by Chamberland and Dilcher [CD09] were expressed as constant terms in (6) and (7), and these representations were deduced in a systematic manner from the defining binomial sums. In general, however, it is an open problem to determine whether a given integer sequence can be represented as a constant term $\operatorname{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$ for Laurent polynomials $P(\boldsymbol{x}), Q(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$. This question was raised by Zagier [Zag18, p. 769, Question 2] and Gorodetsky [Gor21] in the case $Q = 1$ and appears in [Str22] for general Q. A classification in the C-finite case was completed in [BSY23] but the general case remains open, including the special cases of hypergeometric

sequences or those with an algebraic generating function (or, even, the intersection of those).

References

[ABD19] Boris Adamczewski, Jason P. Bell, and Éric Delaygue. Algebraic independence of G-functions and congruences "à la Lucas". *Annales Scientifiques de l'École Normale Supérieure*, 52(3):515–559, 2019.

[And99] George E. Andrews. q-analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher. *Discrete Mathematics*, 204(1):15–25, 1999.

[AvSZ11] Gert Almkvist, Duco van Straten, and Wadim Zudilin. Generalizations of Clausen's formula and algebraic transformations of Calabi–Yau differential equations. *Proceedings of the Edinburgh Mathematical Society*, 54(2):273–295, 2011.

[BSY23] Alin Bostan, Armin Straub, and Sergey Yurkevich. On the representability of sequences as constant terms. *Journal of Number Theory*, 253:235–256, 2023.

[CD06] Marc Chamberland and Karl Dilcher. Divisibility properties of a class of binomial sums. *Journal of Number Theory*, 120(2):349–371, October 2006.

[CD09] Marc Chamberland and Karl Dilcher. A binomial sum related to Wolstenholme's theorem. *Journal of Number Theory*, 129(11):2659–2672, November 2009.

[Del18] Eric Delaygue. Arithmetic properties of Apéry-like numbers. *Compositio Mathematica*, 154(2):249–274, February 2018.

[Ges82] Ira M. Gessel. Some congruences for Apéry numbers. *Journal of Number Theory*, 14(3):362–368, June 1982.

[Gor21] Ofir Gorodetsky. New representations for all sporadic Apéry-like sequences, with applications to congruences. *Experimental Mathematics*, 2021.

[Gra97] Andrew Granville. Arithmetic properties of binomial coefficients I: Binomial coefficients modulo prime powers. *CMS Conference Proceedings*, 20:253–275, 1997.

[HS22] Joel A. Henningsen and Armin Straub. Generalized Lucas congruences and linear p-schemes. *Advances in Applied Mathematics*, 141:#102409, 20 p., 2022.

[Kou09] Christoph Koutschan. *Advanced Applications of the Holonomic Systems Approach*. PhD thesis, RISC, Johannes Kepler University, Linz, Austria, September 2009.

[Luc78] Edouard Lucas. Sur les congruences des nombres Eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier. *Bulletin de la Société Mathématique de France*, 6:49–54, 1878.

[McI92] Richard J. McIntosh. A generalization of a congruential property of Lucas. *American Mathematical Monthly*, 99(3):231–238, March 1992.

[Me4] Romeo Meštrović. Lucas' theorem: its generalizations, extensions and applications (1878–2014). *Preprint*, September 2014. arXiv:1409.3820.

[MS16] Amita Malik and Armin Straub. Divisibility properties of sporadic Apéry-like numbers. *Research in Number Theory*, 2(1):#5, 26 p., 2016.

[MV16] Anton Mellit and Masha Vlasenko. Dwork's congruences for the constant terms of powers of a Laurent polynomial. *International Journal of Number Theory*, 12(2):313–321, 2016.

[OEI25] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences, 2025. Published electronically at https://oeis.org.

[Row22] Eric Rowland. Lucas' theorem modulo p^2. *American Mathematical Monthly*, 129(9):846–855, 2022.

[RY15] Eric Rowland and Reem Yassawi. Automatic congruences for diagonals of rational functions. *Journal de Théorie des Nombres de Bordeaux*, 27(1):245–288, 2015.

[RYK21] Eric Rowland, Reem Yassawi, and Christian Krattenthaler. Lucas congruences for the Apéry numbers modulo p^2. *Integers*, 21(A20):1–15, 2021.

[RZ14] Eric Rowland and Doron Zeilberger. A case study in meta-automation: automatic generation of congruence automata for combinatorial sequences. *Journal of Difference Equations and Applications*, 20(7):973–988, 2014.

[Sch93] Rolf Schneider. *Convex Bodies: The Brunn-Minkowski Theory*, volume 44 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993.

[Str14] Armin Straub. Multivariate Apéry numbers and supercongruences of rational functions. *Algebra & Number Theory*, 8(8):1985–2008, 2014.

[Str22] Armin Straub. On congruence schemes for constant terms and their applications. *Research in Number Theory*, 8(3):#42, 21 p., 2022.

[SvS15] Kira Samol and Duco van Straten. Dwork congruences and reflexive polytopes. *Annales mathématiques du Québec*, 39(2):185–203, October 2015.

[Zag18] Don B. Zagier. The arithmetic and topology of differential equations. In Volker Mehrmann and Martin Skutella, editors, *Proceedings of the European Congress of Mathematics, Berlin, 18-22 July, 2016*, pages 717–776. EMS Press, Berlin, 2018.