Generalized Lucas congruences and linear p-schemes

Joel A. Henningsen [*] Armin Straub [†]

November 16, 2021

Abstract

We observe that a sequence satisfies Lucas congruences modulo p if and only if its values modulo p can be described by a linear p-scheme, as introduced by Rowland and Zeilberger, with a single state. This simple observation suggests natural generalizations of the notion of Lucas congruences. To illustrate this point, we prove explicit generalized Lucas congruences for integer sequences that can be represented as the constant terms of $P(x,y)^n Q(x,y)$ where P and Q are certain Laurent polynomials.

1 Introduction

Throughout this paper, let p be a prime. We say that a sequence $A(n)$ satisfies the *Lucas congruences* modulo p if, for all $n \in \mathbb{Z}_{\geq 0}$,

$$A(n) \equiv A(n_0)A(n_1)\cdots A(n_r) \pmod{p}, \tag{1}$$

where $n = n_0 + n_1 p + \cdots + n_r p^r$ is the expansion of n in base p (in the case $n = 0$, the right-hand side is the empty product so that (1) specializes to $A(0) \equiv 1$). These congruences are named after Lucas [Luc78] who showed such congruences for the binomial coefficients. Since then, Lucas congruences have received considerable attention in the literature and many authors have shown that certain sequences satisfy the Lucas congruences. We refer to [McI92], [Gra97], [SvS15], [MS16], [Del18], [ABD19], [Gor21] and the references therein for recent results of a more general nature as well as more background and details. A historical survey of Lucas-type congruences can be found in [Mes14].

Rowland and Zeilberger [RZ14] recently introduced the notion of *linear p-schemes* to efficiently describe certain sequences $A(n)$ modulo prime powers. Namely, given a sequence $A : \mathbb{Z}_{\geq 0} \to \mathbb{Z}$, a linear p-scheme for $A(n) \pmod{p^r}$

[*] Department of Mathematics and Statistics, University of South Alabama
Current affiliation: Department of Mathematics, Baylor University
[†] Department of Mathematics and Statistics, University of South Alabama
Email: straub@southalabama.edu

consists of *states* $A_0, A_1, \ldots, A_m : \mathbb{Z}_{\geq 0} \to \mathbb{Z}$ with $A_0(n) = A(n)$ such that, for all $i \in \{0, 1, \ldots, m\}$, $k \in \{0, 1, \ldots, p-1\}$ and $n \geq 0$,

$$A_i(pn + k) \equiv \sum_{j=0}^{m} \alpha_{i,j}^{(k)} A_j(n) \pmod{p^r} \tag{2}$$

for some integers $\alpha_{i,j}^{(k)}$. Note that this linear p-scheme has $m+1$ states and is fully determined by the values $\alpha_{i,j}^{(k)}$ together with the initial conditions $c_i = A_i(0)$, all modulo p^r. Rowland and Zeilberger [RZ14] describe algorithms to automatically obtain such a linear p-scheme, for fixed p^r, for any sequence $A(n)$ expressible as *constant terms*, meaning that

$$A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})], \tag{3}$$

where $P, Q \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ are Laurent polynomials in $\boldsymbol{x} = (x_1, \ldots, x_d)$, and $\mathrm{ct}[f(\boldsymbol{x})]$ denotes the constant term of the Laurent polynomial $f(\boldsymbol{x})$. Previously, Rowland and Yassawi [RY15] had described similar algorithms for sequences that are diagonals of multivariate rational functions. We also note that $A(n) \pmod{p^r}$ can be described by a linear p-scheme, as above, if and only if $A(n) \pmod{p^r}$ is p-automatic. In general, linear p-schemes over a ring R represent p-regular sequences [AS92, Theorem 2.2(d)]; if R is finite (as is the case for our considerations, since $R = \mathbb{Z}/p^r\mathbb{Z}$), p-regular sequences coincide with p-automatic sequences [AS92, Theorem 2.3].

Example 1.1. The Catalan numbers $C(n)$ have the constant term expression

$$C(n) = \mathrm{ct}[(x^{-1} + 2 + x)^n (1 - x)]. \tag{4}$$

Based on (4), the algorithm of Rowland and Zeilberger [RZ14] can be used to construct linear p-schemes that describe the Catalan numbers modulo any fixed prime power. For instance, we find the following 2-state linear 3-scheme describing $C(n)$ modulo 3:

$$\begin{aligned} A_0(3n) &= A_1(n) & \qquad A_1(3n) &= A_1(n) \\ A_0(3n+1) &= A_1(n) & \qquad A_1(3n+1) &= 2A_1(n) \\ A_0(3n+2) &= A_0(n) + A_1(n) & \qquad A_1(3n+2) &= 0 \end{aligned}$$

Together with the initial conditions $A_0(0) = A_1(0) = 1$, this scheme uniquely describes all the values taken by the sequences A_0, A_1 and, therefore, the Catalan numbers $C(n) \equiv A_0(n)$ modulo 3. (On the other hand, Example 5.5 offers a more transparent characterization of the Catalan numbers modulo 3.)

Remark 1.2. We note that all constant term representations claimed in this paper can be algorithmically proven using, for instance, creative telescoping [Kou09]. We refer to [Gor21] for worked out examples of this approach.

In the following, we make the rather simple observation that a sequence satisfies the Lucas congruences modulo p if and only if its values modulo p can be encoded by a linear p-scheme with exactly one state.

Proposition 1.3. *Suppose that $A(0) = 1$. Then the sequence $A(n)$ satisfies the Lucas congruences (1) modulo p if and only if the values $A(n)$ modulo p can be encoded by a linear p-scheme with a single state.*

Proof. Recall that, by definition, a single-state linear p-scheme for $A(n)$ modulo p consists of the single state $A_0(n) \equiv A(n) \pmod{p}$ and has the property that, for all $k \in \{0, 1, \ldots, p-1\}$ and $n \geq 0$,

$$A_0(pn + k) \equiv \alpha_{0,0}^{(k)} A_0(n) \pmod{p}.$$

Setting $n = 0$ in this relation and using that $A(0) = 1$, we see that we necessarily have $\alpha_{0,0}^{(k)} = A_0(k)$. The relation therefore becomes $A(pn + k) \equiv A(k)A(n) \pmod{p}$, which is equivalent to the Lucas congruences (1) modulo p. □

Proposition 1.3 places the notion of Lucas congruences in a larger context. In particular, it suggests generalizations such as the following: one might say that a sequence satisfies an order k version of the Lucas congruences if its values modulo p can be encoded by a linear p-scheme with k states.

In Section 4, to illustrate this point, we prove such generalized Lucas congruences of order 2 in Corollary 4.5 (see Remark 4.6). We obtain these as a special case of Theorem 4.1 which itself provides generalized Lucas congruences of order up to 4 for certain constant terms $A(n) = \mathrm{ct}[P(x, y)^n Q(x, y)]$. Another way to interpret these results is as explicitly describing linear p-schemes for these sequences modulo all primes p at the same time (whereas a usual application of the algorithms of Rowland and Zeilberger [RZ14] provides such schemes for fixed p). In Section 5, we apply Theorem 4.1 to the case of the Catalan numbers (4).

In preparation for proving the results of Section 4, we review generalized central trinomial numbers in Section 3. First, however, in Section 2, we review, and give a simple proof of, the following fundamental result which is remarkably effective in proving that certain sequences satisfy Lucas congruences.

Theorem 1.4. *Let $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ be such that its Newton polytope has the origin as its only interior integral point. Then $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ satisfies the Lucas congruences (1) for any prime p.*

Theorem 1.4 is a special case of a result of Samol and van Straten [SvS15] (as well as Mellit and Vlasenko [MV16]), which shows that, if the Newton polytope of $P(\boldsymbol{x})$ has the origin as its only interior integral point, then $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ satisfies the *Dwork congruences*

$$A(p^r m + n)A(\lfloor n/p \rfloor) \equiv A(p^{r-1} m + \lfloor n/p \rfloor)A(n) \pmod{p^r} \tag{5}$$

for all primes p and all integers $m, n \geq 0$, $r \geq 1$. The case $r = 1$ of these congruences is equivalent to the Lucas congruences (1). As such, Theorem 1.4 is a weaker result but, as we show in Section 2, it can be proved much more directly. Moreover, the proof can readily be generalized in other directions. For instance, in Theorem 4.1, we provide generalized Lucas congruences for certain

sequences expressible as $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n Q(\boldsymbol{x})]$. It would be interesting to know whether these sequences satisfy generalized versions of the Dwork congruences (5).

We also note that Rowland and Yassawi [RY15, Theorem 5.2] provide a rather general result in the spirit of Theorem 1.4 for diagonals of certain rational functions.

2 Lucas congruences for constant terms

In the sequel, we will use the vector notation $\boldsymbol{x} = (x_1, \ldots, x_d)$ and write, for instance, $\mathbb{Z}[\boldsymbol{x}^{\pm 1}] = \mathbb{Z}[x_1^{\pm 1}, \ldots, x_d^{\pm 1}]$ for the ring of Laurent polynomials in d variables with integer coefficients. We denote monomials as $\boldsymbol{x}^{\boldsymbol{k}} = x_1^{k_1} \cdots x_d^{k_d}$, where $\boldsymbol{k} = (k_1, \ldots, k_d)$ is the exponent vector. If $f(\boldsymbol{x}) = \sum a_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ is a Laurent polynomial, then $\mathrm{supp}(f) \subseteq \mathbb{Z}^d$ denotes the support of f, consisting of those $\boldsymbol{k} \in \mathbb{Z}^d$ for which $a_{\boldsymbol{k}} \neq 0$. For such f, we also use the common notation $[\boldsymbol{x}^{\boldsymbol{k}}][f(\boldsymbol{x})] = a_{\boldsymbol{k}}$. The Newton polytope of f is the convex hull of $\mathrm{supp}(f)$. We further denote with Λ_p the Cartier operator

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

In this section, we give a short proof of Theorem 1.4, copied below as Theorem 2.1, which is instructive for the generalized Lucas congruences that we consider in Section 4. In the remainder of this section, we then illustrate the versatility of Theorem 2.1 by giving several examples.

Theorem 2.1. *Let $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ be such that its Newton polytope has the origin as its only interior integral point. Then $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ satisfies the Lucas congruences (1) for any prime p.*

Proof. Let $n \geq 0$ and $k \in \{0, 1, \ldots, p-1\}$. We have

$$\begin{aligned} A(pn+k) &= \mathrm{ct}[P(\boldsymbol{x})^{pn} P(\boldsymbol{x})^k] \\ &\equiv \mathrm{ct}[P(\boldsymbol{x}^p)^n P(\boldsymbol{x})^k] \pmod{p} \\ &= \mathrm{ct}[P(\boldsymbol{x})^n \Lambda_p[P(\boldsymbol{x})^k]], \end{aligned} \tag{6}$$

where we used that $P(\boldsymbol{x})^{pn} \equiv P(\boldsymbol{x}^p)^n$ modulo p. Write $\mathrm{supp}(P) = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_t\}$. In other words, let $\boldsymbol{v}_i$ be the exponents of terms of $P(\boldsymbol{x})$. Suppose that $c\boldsymbol{x}^{\boldsymbol{v}}$, with $c \neq 0$, is a term of $\Lambda_p[P(\boldsymbol{x})^k]$. This is equivalent to $c\boldsymbol{x}^{p\boldsymbol{v}}$ being a term of $P(\boldsymbol{x})^k$, which implies that

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

where $\lambda_i \in \mathbb{Z}_{\geq 0}$ and $\lambda_1 + \lambda_2 + \cdots + \lambda_t = k$. It follows that

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

where $\mu_i \geq 0$ and $\mu_1 + \cdots + \mu_t = k/p < 1$, which shows that $\boldsymbol{v}$ is an interior point of the Newton polytope of $P(\boldsymbol{x})$. By assumption, it must be that $\boldsymbol{v} = \mathbf{0}$. Consequently, $\Lambda_p[P(\boldsymbol{x})^k] = \mathrm{ct}[P(\boldsymbol{x})^k]$. Combined with (6), we conclude that

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

as claimed. □

Since it is particularly convenient to apply in practice, we record the following special case of Theorem 2.1.

Corollary 2.2. *Let $P \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ and suppose that $\mathrm{supp}(P) \subseteq \{-1, 0, 1\}^d$. Then $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ satisfies the Lucas congruences (1) for any prime p.*

We note that the case $d = 2$ can also be obtained as a special case of Theorem 4.1 offered in the next section.

Example 2.3. It is immediate from Corollary 2.2 that the central binomial coefficients

$$\binom{2n}{n} = \mathrm{ct}\left[\frac{(1+x)^{2n}}{x^n}\right] = \mathrm{ct}\left[\left(\frac{1}{x} + 2 + x\right)^n\right] \tag{7}$$

satisfy the Lucas congruences modulo any prime. In the same manner, it follows from Corollary 2.2 that the central trinomial coefficients

$$T(n) = \mathrm{ct}[(x^{-1} + 1 + x)^n]$$

satisfy the Lucas congruences as well. This is [DS06, Theorem 4.7] and, as recorded in Corollary 3.1, the result extends directly to the generalized trinomial coefficients.

Example 2.4. The sequences

$$A_s(n) = \sum_{k_1 + \cdots + k_s = n} \binom{n}{k_1, \ldots, k_s}^2$$

count abelian squares [RS09], which are strings of length $2n$ where the second half is a permutation of the first, over an alphabet with s letters. The numbers $A_s(n)$ are also the $2n$-th moments of the distance travelled by an s-step random walk in the plane [BNSW11], where each step is of unit length and taken in a uniformly chosen random direction. As observed in [BNSW11, (8)], we have the constant term representation

$$\begin{aligned} A_s(n) &= \mathrm{ct}[((x_1 + \cdots + x_s)(x_1^{-1} + \cdots + x_s^{-1}))^n] \\ &= \mathrm{ct}[((1 + x_1 + \cdots + x_{s-1})(1 + x_1^{-1} + \cdots + x_{s-1}^{-1}))^n]. \end{aligned}$$

Applying Corollary 2.2 to these constant terms, we are able to conclude that, for each positive integer s, the sequence $A_s(n)$ satisfies the Lucas congruences modulo any prime.

Example 2.5. Based on the binomial sum representation

$$A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \tag{8}$$

Gessel [Ges82, Theorem 1] proved that the Apéry numbers $A(n)$ satisfy the Lucas congruences. This result can also be obtained as an immediate consequence of Corollary 2.2 in light of the constant term representation [Str14, Remark 1.4]

$$A(n) = \mathrm{ct}\left[\frac{(x+y)(z+1)(x+y+z)(y+z+1)}{xyz}\right]^n.$$

We note that the Apéry numbers (8) were introduced by R. Apéry in his surprising proof [Apé79], [Poo79] of the irrationality of $\zeta(3)$. One of their, at the time unexpected, properties is that they satisfy a certain type of three-term recurrence. It remains an open problem to classify the integer sequences which satisfy recurrences of this shape. It is believed that, essentially, there are only finitely many such sequences and, presently, 15 such sporadic Apéry-like sequences have been found by Zagier [Zag09], Almkvist, Zudilin [AZ06] and Cooper [Coo12] in extensive computer searches. Malik and the second author [MS16] proved that all of these 15 sequences satisfy Lucas congruences. In 13 of these cases, they were able to follow McIntosh's approach [McI92] of establishing Lucas congruences based on suitable representations as binomials sums. On the other hand, considerably more analysis was needed to handle the remaining two cases (labelled (η) and s_{18}). More recently, Gorodetsky [Gor21] was able to simplify the proof of the Lucas congruences by obtaining suitable constant term representations for each Apéry-like sporadic sequences. In 14 cases (all except (η)), these constant term expressions are of the form $A(n) = \mathrm{ct}[P(\boldsymbol{x})^n]$ where the Newton polytope of $P(\boldsymbol{x})$ has the origin as its only interior integral point. Using Theorem 2.1, it therefore follows that these 14 sequences satisfy the Lucas congruences.

We conclude this section by considering the sequence

$$S(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n-k}{k}.$$

Presumably based on numerical values, Z.-W. Sun [Slo21, A275027] conjectured that $S(n) \equiv 0, \pm 1 \pmod 5$. As another application of Theorem 2.1, we prove this claim by showing that the sequence $S(n)$ satisfies Lucas congruences.

Lemma 2.6. *For all $n \in \mathbb{Z}_{\geq 0}$, we have, modulo 5,*

$$S(n) \equiv \begin{cases} (-1)^{d(n)}, & \text{if the digits of } n \text{ in base } 5 \text{ are all } 0, 1, 3, \\ 0, & \text{otherwise,} \end{cases}$$

where $d(n)$ is the number of digits of n in base 5 that are equal to 3.

Proof. We first express $S(n)$ as constant terms by following the procedure outlined in [RZ14] for converting certain binomial sums to constant terms:

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

It follows immediately from this expression and Corollary 2.2 that $S(n)$ satisfies the Lucas congruences (1) modulo any prime.

The claim then follows from the initial values of $S(n)$ modulo 5:

$$S(0) \equiv 1, \quad S(1) \equiv 1, \quad S(2) \equiv 0, \quad S(3) \equiv -1, \quad S(4) \equiv 0 \pmod 5$$

□

In [Slo21, A275027] it is further observed that $S(n)$ is always odd and that this can be seen from the alternative binomial sum

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

combined with the fact that $\binom{2k}{k} = 2\binom{2k-1}{k-1}$ for $k = 1, 2, \ldots$ We note that such statements are particularly easy to understand in terms of Lucas congruences. In this instance, it follows from $S(0) = S(1) = 1$, together with the Lucas congruences modulo 2, that $S(n)$ is always odd. More generally, it follows from the Lucas congruences that $S(n)$ is never divisible by a prime p if none of the values $S(0), S(1), \ldots, S(p-1)$ is divisible by p. By direct computation, this allows us to conclude that $S(n)$ is never divisible by the following primes:

$$2, 3, 7, 11, 31, 41, 67, 73, 79, 89, 97, \ldots$$

It would be interesting, but appears to be much more difficult, to explicitly characterize those primes.

3 Generalized central trinomial numbers

Noe [Noe06] studied the generalized central trinomial numbers

$$T(n) = \operatorname{ct}[(ax^{-1} + b + cx)^n] = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} \binom{2k}{k} (ac)^k b^{n-2k},$$

which generalize the classical case $a = b = c = 1$ already considered by Euler. As another immediate application of Corollary 2.2, we obtain the following

result, which is also proved by Noe [Noe06, (13)] using a congruence of Schur for Legendre polynomials, and by Deutsch and Sagan [DS06, Theorem 4.7] in the case $a = b = c = 1$.

Corollary 3.1. *The generalized central trinomial numbers $T(n)$ satisfy the Lucas congruences (1) for any prime p.*

Among further divisibility properties, Noe [Noe06, Theorem 8.8] determines $T(p-1)$ modulo p as follows. For $d \in \mathbb{Z}$, let (d/p) denote the Kronecker symbol so that, for odd primes p, we have $(d/p) \equiv d^{(p-1)/2} \pmod{p}$ while, for $p = 2$, we simply have $(d/2) \equiv d \pmod{2}$.

Lemma 3.2. *For all primes p and integers a, b, c,*

$$\operatorname{ct}[(ax^{-1} + b + cx)^{p-1}] \equiv \left(\frac{b^2 - 4ac}{p}\right) \pmod{p}.$$

Proof. For odd primes, Noe [Noe06, Theorem 8.8] deduces this result from the congruences

$$T(p-k-1) \equiv d^{(p-1)/2-k} T(k) \pmod{p}, \quad d = b^2 - 4ac,$$

for the generalized trinomial coefficients, which in turn follow from the congruences $P_{p-k-1}(x) \equiv P_k(x)$ for the corresponding Legendre polynomials due to Holt.

On the other hand, for $p = 2$, we have $\operatorname{ct}[(ax^{-1} + b + cx)^{p-1}] = b$ as well as $b \equiv b^2 \equiv d \equiv (d/p) \pmod{2}$ so that the result is trivially true. □

We will also need the following variation.

Lemma 3.3. *If p is an odd prime and $c \not\equiv 0 \pmod{p}$, then*

$$\operatorname{ct}[(ax^{-1} + b + cx)^{p-1} x] \equiv \frac{b}{2c}\left(1 - \left(\frac{b^2 - 4ac}{p}\right)\right) \pmod{p}.$$

If $p = 2$ or $c \equiv 0 \pmod{p}$, then we have this congruence with the right-hand replaced by $-ab^{p-2}$ (which is understood to be a if $p = 2$).

Proof. Note that

$$\operatorname{ct}[(ax^{-1} + b + cx)^n ax^{-1}] = \operatorname{ct}[(cx + b + ax^{-1})^n cx]$$

upon replacing x by ax^{-1}/c (which does not affect the value of the constant term). Consequently,

$$\begin{aligned} T(n+1) &= \operatorname{ct}[(ax^{-1} + b + cx)^n (ax^{-1} + b + cx)] \\ &= bT(n) + 2\operatorname{ct}[(ax^{-1} + b + cx)^n x] \end{aligned}$$

so that, if $p \neq 2$ and $c \not\equiv 0 \pmod{p}$,

$$\operatorname{ct}[(ax^{-1} + b + cx)^n x] = \frac{1}{2c}(T(n+1) - bT(n)). \tag{9}$$

In this case, the claim therefore follows from Lemma 3.2 combined with $T(p) \equiv 1 \pmod p$, which is a consequence of the fact that $T(n)$ satisfies the Lucas congruences, see Corollary 3.1.

The case $p = 2$ is trivial because $\mathrm{ct}[(ax^{-1} + b + cx)x] = a$. On the other hand, if $c \equiv 0 \pmod p$, then $\mathrm{ct}[(ax^{-1} + b + cx)^{p-1}x] = (p-1)ab^{p-2} \equiv -ab^{p-2} \pmod p$. □

4 Generalized Lucas congruences

The following result, Theorem 4.1, is the main technical result of this paper and provides generalized Lucas congruences (10) for certain constant terms $A(n) = \mathrm{ct}[P(x,y)^n Q(x,y)]$. The result is somewhat involved to state in full generality but a simpler special case is spelled out in Corollary 4.5 below. Note that it follows from Corollary 2.2 that the sequence $B(n)$ in Theorem 4.1 satisfies the ordinary Lucas congruences (1), while the sequence $\tilde{A}(n)$ in (10) is such that Theorem 4.1 again applies to provide generalized Lucas congruences (10) (with the same values for σ_x, σ_y and $\hat{Q}(x,y)$). As a result, the congruences (10) are sufficient to determine all values of $A(n)$ modulo any prime p (from the first p values of each of the involved sequences).

Theorem 4.1. *Let $A(n) = \mathrm{ct}[P(x,y)^n Q(x,y)]$ where $P, Q \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$ with*

$$P(x,y) = \sum_{(i,j)\in\{-1,0,1\}^2} a_{i,j} x^i y^j, \quad Q(x,y) = \alpha + \beta x + \gamma y + \delta xy.$$

Then, for any $n \in \mathbb{Z}_{\geq 0}$ and $k \in \{0, 1, \ldots, p-1\}$,

$$A(pn+k) \equiv B(n)A(k) + \begin{cases} 0, & \text{if } k < p-1, \\ \tilde{A}(n), & \text{if } k = p-1, \end{cases} \pmod p. \tag{10}$$

Here, $B(n) = \mathrm{ct}[P(x,y)^n]$ and $\tilde{A}(n) = \mathrm{ct}[P(x,y)^n \tilde{Q}(x,y)]$ with

$$\tilde{Q}(x,y) = Q(\sigma_x x, \sigma_y y) - \alpha + \delta \hat{Q}(x,y),$$

where the quantities $\sigma_x, \sigma_y \in \{0, \pm 1\}$ are given by

$$\sigma_x = \left(\frac{a_{1,0}^2 - 4a_{1,-1}a_{1,1}}{p}\right), \quad \sigma_y = \left(\frac{a_{0,1}^2 - 4a_{-1,1}a_{1,1}}{p}\right), \tag{11}$$

and

$$\hat{Q}(x,y) = \frac{a_{1,0}}{2a_{1,1}}(1-\sigma_x)x + \frac{a_{0,1}}{2a_{1,1}}(1-\sigma_y)y + (1-\sigma_x\sigma_y)xy$$

provided that p is odd and $p \nmid a_{1,1}$. If $p = 2$ or $p | a_{1,1}$, then

$$\hat{Q}(x,y) = -a_{1,-1}a_{1,0}^{p-2}x - a_{-1,1}a_{0,1}^{p-2}y + (a_{1,1} - \sigma_x\sigma_y)xy$$

with the understanding that, if $p = 2$, then $a^{p-2} = 1$ for any integer a.

Proof. As for (6) in the beginning of the proof of Theorem 2.1, we find

$$\begin{aligned} A(pn+k) &= \operatorname{ct}[P(x,y)^{pn+k}Q(x,y)] \\ &\equiv \operatorname{ct}[P(x^p,y^p)^n P(x,y)^k Q(x,y)] \pmod p \\ &= \operatorname{ct}[P(x,y)^n \Lambda_p[P(x,y)^k Q(x,y)]] \\ &= \operatorname{ct}[P^n \Lambda_p[P^k Q]]. \end{aligned} \tag{12}$$

If $k < p-1$, then $\Lambda_p[P^kQ] = \operatorname{ct}[P^kQ]$ because the degree, in x or y or their inverses, of each term of P^kQ is bounded by $k+1<p$. In that case, we thus get

$$A(pn+k) \equiv \operatorname{ct}[P^n]\operatorname{ct}[P^kQ] = B(n)A(k) \pmod p.$$

In the remainder, we therefore consider the case $k = p-1$.

$$\begin{aligned} \Lambda_p[P^{p-1}Q] &= \operatorname{ct}[P^{p-1}Q] + \sum_{T\in\{x,y,xy\}} T\cdot[T^p][P^{p-1}Q] \\ &= A(p-1) + \sum_{T\in\{x,y,xy\}} T\cdot \operatorname{ct}\left[\left(\frac{P}{T}\right)^{p-1}\frac{Q}{T}\right] \end{aligned} \tag{13}$$

For $T=xy$, we obtain

$$\operatorname{ct}\left[\left(\frac{P}{xy}\right)^{p-1}\frac{Q}{xy}\right] = a_{1,1}^{p-1}\delta$$

because all nonconstant terms of the polynomial inside the constant term on the left-hand side feature x and y with negative exponents. Similarly, for $T=x$, we have

$$\operatorname{ct}\left[\left(\frac{P}{x}\right)^{p-1}\frac{Q}{x}\right] = \operatorname{ct}[(a_{1,-1}y^{-1}+a_{1,0}+a_{1,1}y)^{p-1}(\beta+\delta y)]$$

because the left-hand side features no terms involving x with positive exponent. We evaluate the right-hand side using Lemmas 3.2 and 3.3, which show that

$$\begin{aligned} \operatorname{ct}[(a_{1,-1}y^{-1}+a_{1,0}+a_{1,1}y)^{p-1}] &\equiv \left(\frac{a_{1,0}^2-4a_{1,-1}a_{1,1}}{p}\right) = \sigma_x \pmod p, \\ \operatorname{ct}[(a_{1,-1}y^{-1}+a_{1,0}+a_{1,1}y)^{p-1}y] &\equiv \frac{a_{1,0}}{2a_{1,1}}(1-\sigma_x) \pmod p, \end{aligned}$$

the latter assuming that p is odd and $p\nmid a_{1,1}$ (we will make this assumption for the remainder of the proof; if $p=2$ or $p|a_{1,1}$ then we only need to use the corresponding evaluation provided by Lemma 3.3 instead). Combining these we therefore have

$$\operatorname{ct}\left[\left(\frac{P}{x}\right)^{p-1}\frac{Q}{x}\right] \equiv \sigma_x\beta + \frac{a_{1,0}}{2a_{1,1}}(1-\sigma_x)\delta \pmod p,$$

and, by the same arguments,

$$\operatorname{ct}\left[\left(\frac{P}{y}\right)^{p-1}\frac{Q}{y}\right] \equiv \sigma_y\gamma + \frac{a_{0,1}}{2a_{1,1}}(1-\sigma_y)\delta \pmod{p}.$$

Using these evaluations in (13), we have shown that

$$\Lambda_p[P^{p-1}Q] \equiv A(p-1) + \tilde{Q}(x,y) \pmod{p},$$

which, applied to (12), allows us to conclude

$$\begin{aligned} A(pn+(p-1)) &\equiv \operatorname{ct}[P^n(A(p-1)+\tilde{Q}(x,y))] \pmod{p} \\ &= B(n)A(p-1)+\tilde{A}(n), \end{aligned}$$

as claimed in (10). □

Example 4.2. If $Q(x,y)=1$ in Theorem 4.1, then $B(n)=A(n)$ as well as $\tilde{A}(n)=0$, so that the generalized Lucas congruences (10) become the familiar Lucas congruences (1) (that these hold follows more easily from Corollary 2.2).

Example 4.3. Consider the sequence

$$A(n) = \operatorname{ct}\left[\left(x+y+\frac{1}{x}-\frac{1}{y}\right)^n (1+x+xy)\right]. \tag{14}$$

One can show, for instance using creative telescoping, see Remark 1.2, that $A(n)$ has the particularly simple closed form

$$A(n) = (-1)^{\lfloor n/2\rfloor+\lfloor n/4\rfloor}\binom{n}{\lfloor n/2\rfloor}\binom{\lfloor n/2\rfloor}{\lfloor n/4\rfloor}. \tag{15}$$

Applying Theorem 4.1 to $A(n)$, we obtain $\sigma_x=\sigma_y=1$ and $\hat{Q}(x,y)=-xy$ so that $\tilde{Q}(x,y)=Q(x,y)-1-xy=x$ and, thus,

$$\tilde{A}(n) = \operatorname{ct}\left[\left(x+y+\frac{1}{x}-\frac{1}{y}\right)^n x\right] = \begin{cases} A(n), & \text{if } n \text{ odd},\\ 0, & \text{if } n \text{ even}, \end{cases} \tag{16}$$

where the latter equality can again be shown automatically using creative telescoping. Similarly,

$$B(n) = \operatorname{ct}\left[\left(x+y+\frac{1}{x}-\frac{1}{y}\right)^n\right] = \begin{cases} A(n), & \text{if } n\equiv 0 \pmod 4,\\ 0, & \text{otherwise.} \end{cases}$$

Using the relations of the sequences $\tilde{A}(n)$ and $B(n)$ to $A(n)$, the generalized Lucas congruences (10) provided by Theorem 4.1 take the simplified form

$$A(pn+k) \equiv \begin{cases} A(n)A(k), & \text{if } n\equiv 0 \pmod 4,\\ A(n), & \text{if } n\equiv 1 \pmod 2 \text{ and } k=p-1,\\ 0, & \text{otherwise,} \end{cases} \pmod{p},$$

where $n\in\mathbb{Z}_{\geq 0}$ and $k\in\{0,1,\ldots,p-1\}$.

Remark 4.4. Note that Theorem 4.1 is sufficient to apply to all cases of constant terms $A(n) = \mathrm{ct}[P(x,y)^n Q(x,y)]$ where $\mathrm{supp}(P), \mathrm{supp}(Q) \subseteq \{-1,0,1\}^2$. To see this, observe that, for instance in the case of the monomial $Q(x,y) = 1/(xy)$, the constant term can be rewritten as

$$\mathrm{ct}[P(x,y)^n/(xy)] = \mathrm{ct}[P(1/x,1/y)^n xy],$$

where the right-hand side is such that Theorem 4.1 applies. In the same way, we can handle the monomials $1/x$, $1/y$ as well as x/y and y/x and, therefore, reduce the cases $\mathrm{supp}(Q) \subseteq \{-1,0,1\}^2$ to $\mathrm{supp}(Q) \subseteq \{0,1\}^2$.

The following is a special case of Theorem 4.1, for which the generalized Lucas congruences (10) take the simplified form (17).

Corollary 4.5. *Let* $A(n) = \mathrm{ct}[P(x,y)^n Q(x,y)]$ *where* $P, Q \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$ *with*

$$P(x,y) = \sum_{(i,j)\in\{-1,0,1\}^2} a_{i,j} x^i y^j, \quad Q(x,y) = \alpha + \beta x + \gamma y + \delta xy.$$

Suppose that $\delta = 0$, *or that both* p *is odd and* $p \nmid a_{1,1}$. *Suppose further that* $\sigma_x = \sigma_y = 1$, *where* σ_x, σ_y *are as in* (11). *Then, for any* $n \in \mathbb{Z}_{\geq 0}$ *and* $k \in \{0,1,\ldots,p-1\}$,

$$A(pn+k) \equiv B(n)A(k) + \begin{cases} 0, & \text{if } k < p-1, \\ A(n) - A(0)B(n), & \text{if } k = p-1, \end{cases} \pmod p. \quad (17)$$

Here, again, $B(n) = \mathrm{ct}[P(x,y)^n]$.

Proof. This is an immediate consequence of Theorem 4.1 because, under the present conditions, we have $\tilde{Q}(x,y) = Q(x,y) - \alpha$ which implies $\tilde{A}(n) = A(n) - \alpha B(n) = A(n) - A(0)B(n)$. □

Remark 4.6. We note that the congruences (17), together with the Lucas congruences $B(pn+k) \equiv B(n)B(k) \pmod p$, form a two-state linear p-scheme (with the states $A_0 = A$, $A_1 = B$) characterizing the sequence $A(n)$ modulo p. In the sense discussed after Proposition 1.3, it is therefore shown by Corollary 4.5 that the sequence $A(n)$ satisfies an order 2 version of the Lucas congruences.

In Lemma 4.7 below, we observe that the congruences (17) are natural consequences of the ordinary Lucas congruences (1) in the sense that, if $B(n)$ is a sequence satisfying (1), then any linear combination $A(n) = \alpha B(n) + \beta B(n+1)$ satisfies the congruences (17). Certain constant terms $A(n) = \mathrm{ct}[P(x,y)^n Q(x,y)]$ can indeed be expressed as linear combinations of $B(n) = \mathrm{ct}[P(x,y)^n]$ and $B(n+1)$ (see, for instance, Example 4.8), in which case Corollary 4.5 can therefore be obtained (more simply) as a consequence of Lemma 4.7. On the other hand, as indicated by Example 4.9, this is not generally the case. It would be of interest to fully characterize the constant terms which are linear combinations of shifts of $B(n)$.

Lemma 4.7. *Suppose that $B(n)$ satisfies the Lucas congruences (1) modulo p. Then, for any $\alpha, \beta \in \mathbb{Z}$, $A(n) = \alpha B(n) + \beta B(n+1)$ satisfies the congruences (17) modulo p.*

Proof. Suppose that $k < p-1$. Then, using the fact that $B(n)$ satisfies the Lucas congruences (1), we have

$$\begin{aligned} A(pn+k) &= \alpha B(pn+k) + \beta B(pn+(k+1)) \\ &\equiv \alpha B(n)B(k) + \beta B(n)B(k+1) \pmod{p} \\ &= B(n)A(k), \end{aligned}$$

as in the congruences (17). On the other hand, let $k = p-1$. Then,

$$\begin{aligned} A(pn+p-1) &= \alpha B(pn+p-1) + \beta B(p(n+1)) \\ &\equiv \alpha B(n)B(p-1) + \beta B(n+1)B(0) \pmod{p}. \end{aligned}$$

Using $B(0) = 1$ and $\alpha B(p-1) = A(p-1) - \beta B(p) \equiv A(p-1) - \beta B(1)$ as well as $\beta B(n+1) = A(n) - \alpha B(n)$, this implies

$$\begin{aligned} A(pn+p-1) &\equiv B(n)[A(p-1) - \beta B(1)] + [A(n) - \alpha B(n)] \pmod{p} \\ &= B(n)A(p-1) + A(n) - B(n)[\alpha + \beta B(1)] \\ &= B(n)A(p-1) + A(n) - B(n)A(0), \end{aligned}$$

so that congruence (17) holds in this case as well. □

Example 4.8. The sequence

$$B(n) = \operatorname{ct}\left[\left(4 + x + y + \frac{1}{x} + \frac{1}{y}\right)^n\right] = \sum_{k=0}^{n} \binom{n}{k}\binom{2k}{k}\binom{2(n-k)}{n-k}$$

is the Apéry-like sequence labeled ***E*** by Zagier [Zag09] (and (d) in [AZ06]). By Corollary 2.2, the sequence $B(n)$ satisfies the Lucas congruences (1). (We refer to the discussion after Example 2.5 for more information on Apéry-like sequences.) It further follows from Corollary 4.5 that the sequence

$$A(n) = \operatorname{ct}\left[\left(4 + x + y + \frac{1}{x} + \frac{1}{y}\right)^n x\right]$$

with initial values $0, 1, 8, 57, 400, 2820, 20064, 144137, \ldots$ satisfies the generalized Lucas congruences (17). In this particular case, this can also be deduced from Lemma 4.7 because of the relation

$$A(n) = \frac{1}{4}B(n+1) - B(n), \tag{18}$$

which follows from the fact that the Laurent polynomial $4 + x + y + x^{-1} + y^{-1}$ is symmetric in x, y, x^{-1}, y^{-1}, so that

$$B(n+1) = 4B(n) + \sum_{T \in \{x, y, x^{-1}, y^{-1}\}} \operatorname{ct}\left[\left(4 + x + y + \frac{1}{x} + \frac{1}{y}\right)^n T\right] = 4(B(n) + A(n))$$

because the contribution from each of the four possibilities for T is the same.

However, as illustrated by the next example, it is not generally the case in Corollary 4.5 that the sequence $A(n)$ is a linear combination of $B(n)$ and $B(n+1)$ as in (18).

Example 4.9. As a variation of the previous example, let us consider, for any integer λ, the sequences

$$A(n) = \mathrm{ct}\left[\left(\lambda + x + y + \frac{1}{x} - \frac{1}{y}\right)^n x\right] = \sum_{\substack{k=0 \\ k\equiv 1\ (2)}}^{n} \lambda^{n-k}\binom{n}{k} D(k),$$

where $D(n)$ is the hypergeometric term (15) and the latter equality is a consequence of (16) and binomially expanding $(\lambda+P)^n$ with $P = x+y+x^{-1}-y^{-1}$. As in the previous example, it follows from Corollary 4.5 that the sequence $A(n)$ satisfies the generalized Lucas congruences (17) with

$$\begin{aligned} B(n) &= \mathrm{ct}\left[\left(\lambda + x + y + \frac{1}{x} - \frac{1}{y}\right)^n\right] = \sum_{\substack{k=0 \\ k\equiv 0\ (4)}}^{n} \lambda^{n-k}\binom{n}{k} D(k) \\ &= \sum_{k=0}^{\lfloor n/4\rfloor} (-1)^k \lambda^{n-4k}\binom{n}{4k}\binom{4k}{2k}\binom{2k}{k}. \end{aligned}$$

In contrast to the previous example, however, the sequence $A(n)$ cannot be written as a linear combination of $B(n)$ and $B(n+1)$ as in (18) (as can be seen, for instance, by comparing initial values).

5 Catalan numbers

As an application, we spell out the univariate special case of Theorem 4.1 which is particularly simple. We then illustrate the result by applying it to the Catalan numbers $C(n)$. In particular, we derive a Lucas-like congruence for $C(n)$ modulo p as a product of terms corresponding to the p-adic digits of n.

Corollary 5.1. *Let $A(n) = \mathrm{ct}[(ax^{-1}+b+cx)^n(\alpha+\beta x)]$ where $a, b, c, \alpha, \beta \in \mathbb{Z}$ with $c \not\equiv 0 \pmod p$. Then the generalized Lucas congruences (17) hold with $B(n) = \mathrm{ct}[(ax^{-1}+b+cx)^n]$.*

Proof. This follows directly from Theorem 4.1 since $\sigma_x = (c^2/p) = 1$ in the present case so that we have, as in Corollary 4.5, $\tilde{Q}(x,y) = Q(x,y) - \alpha$ and, therefore, $\tilde{A}(n) = A(n) - A(0)B(n)$.

Alternatively, for odd p, the result is a special case of Lemma 4.7 because, as observed in (9),

$$\mathrm{ct}[(ax^{-1}+b+cx)^n x] = \frac{1}{2c}(B(n+1) - bB(n)),$$

so that

$$A(n) = \frac{\beta}{2c}B(n+1) + \left(\alpha - \frac{b\beta}{2c}\right)B(n).$$

□

Example 5.2. The case $c = 0$ in Corollary 5.1 needs to be excluded since, in that case, $A(n) = \alpha b^n + a\beta n b^{n-1}$ while $B(n) = b^n$. However, Theorem 4.1 still applies (now $\sigma_x = 0$ so that $\tilde{Q}(x, y) = 0$ and $\tilde{A}(n) = 0$) to show that, for any $n \in \mathbb{Z}_{\geq 0}$ and $k \in \{0, 1, \ldots, p-1\}$, we have the congruences

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

which are straightforward to verify directly using Fermat's little theorem.

Recall from (4) that the Catalan numbers have the constant term expression $C(n) = \mathrm{ct}[(x^{-1} + 2 + x)^n(1 - x)]$.

Corollary 5.3. *Let $C(n)$ be the Catalan numbers. Modulo p,*

$$C(pn + k) \equiv \begin{cases} \binom{2n}{n} C(k), & \text{if } k < p - 1, \\ -(2n + 1)C(n), & \text{if } k = p - 1. \end{cases}$$

Proof. As noted in (7), $\mathrm{ct}[(x^{-1} + 2 + x)^n]$ are the central binomial coefficients. Since $C(0) = 1$, Corollary 5.1 thus shows that, modulo p,

$$C(pn + k) \equiv \binom{2n}{n} C(k) + \begin{cases} 0, & \text{if } k < p - 1, \\ C(n) - \binom{2n}{n}, & \text{if } k = p - 1. \end{cases}$$

In the case $k = p - 1$, it follows from Lemmas 3.2 and 3.3 that $C(p - 1) \equiv -1 \pmod{p}$, which implies

$$\binom{2n}{n} C(p-1) + C(n) - \binom{2n}{n} \equiv C(n) - 2\binom{2n}{n} = -(2n + 1)C(n) \pmod{p},$$

as claimed. □

By iterating Corollary 5.3 and combining it with the Lucas congruences for the central binomial coefficients, we obtain the following equivalent result which spells out generalized Lucas congruences for the Catalan numbers in a form similar to (1).

Corollary 5.4. *Suppose the p-adic digits of n are $p-1, \ldots, p-1, n_0, n_1, \ldots, n_r$ with m initial digits that are $p - 1$ and $n_0 \neq p - 1$. Then we have*

$$C(n) \equiv \delta(n_0, m) C(n_0) \binom{2n_1}{n_1} \cdots \binom{2n_r}{n_r} \pmod{p}, \tag{19}$$

where $\delta(n_0, m) = 1$ if $m = 0$ and $\delta(n_0, m) = -(2n_0 + 1)$ if $m \geq 1$.

Corollary 5.4 is not difficult to establish directly (though we have not been able to find it explicitly stated in the literature): in particular, the case $m = 0$ (equivalently, $n \not\equiv -1 \pmod{p}$) is obvious from the Lucas congruences for the central binomial coefficients combined with the representation $C(n) = \frac{1}{n+1}\binom{2n}{n}$. On the other hand, we obtained Corollary 5.4 in a simple and natural manner, as a very special case of Theorem 4.1 which applies to many other sequences of combinatorial and number theoretic interest.

Example 5.5. The generalized Lucas congruences make certain properties of a sequence particularly transparent. For instance, for the Catalan numbers, Deutsch and Sagan [DS06, Theorem 5.2] prove that

$$C(n) \equiv \begin{cases} (-1)^{\delta_3^*(n+1)}, & \text{if } n+1 \in T^*(01), \\ 0, & \text{otherwise,} \end{cases} \pmod 3,$$

where $T^*(01)$ consists of those integers $m \geq 0$ whose ternary expansion $m = m_0 + 3m_1 + 3^2 m_2 + \ldots$ is such that $m_i \in \{0, 1\}$ for all $i \geq 1$ while, in terms of this expansion, $\delta_3^*(m)$ is the number of m_i with $i \geq 1$ such that $m_i = 1$.

We observe that this characterization of the Catalan numbers modulo 3 follows directly from Corollary 5.4, the only work consisting in transcribing the notations: indeed, notice that $C(n_0) = 1$ in (19) (because $C(0) = C(1) = 1$) while $\binom{2n_i}{n_i}$ is $1, -1$, or 0 modulo 3 depending on whether n_i is $0, 1$, or 2, respectively. We thus see from (19) that $C(n)$ is divisible by 3 if and only if $m \geq 1$ and $n_0 = 1$ (in that case $\delta(n_0, m) = 0$), or if one of the $n_1, n_2, \ldots$ is 2. This is equivalent to $n + 1 \notin T^*(01)$. In the same manner, we can see that $C(n) \equiv (-1)^{\delta_3^*(n+1)} \pmod 3$ if $n + 1 \in T^*(01)$.

Example 5.6. To emphasize the point of the previous example, we use Corollary 5.4 to produce a similar result for the Catalan numbers modulo 5:

$$C(n) \equiv \begin{cases} 2^{\lambda(n)}, & \text{if } n \notin Z, \\ 0, & \text{otherwise,} \end{cases} \pmod 5,$$

where, using the notation of Corollary 5.4, the set Z consists of those integers $n \geq 0$ satisfying $n_0 = 3$, or $n_i \in \{3, 4\}$ for some $i \geq 1$, or both $n_0 = 2$ and $m \geq 1$. The exponent $\lambda(n)$ is the number of $n_1, n_2, \ldots$ equal to 1; and $\lambda(n)$ is increased by 1 if $n_0 = 2$, or if both $n_0 = 1$ and $m \geq 1$, while $\lambda(n)$ is increased by 2 if both $n_0 = 0$ and $m \geq 1$. Though effective, we invite the reader to translate this description into a more pleasing form.

6 Conclusion

Theorem 4.1 characterizes all sequences $A(n)$ modulo p which can be expressed as the constant terms of $P(x, y)^n Q(x, y)$ for Laurent polynomials P and Q that are linear in each of x, y, x^{-1}, y^{-1}. Though we have not pursued this line of inquiry here, one could follow the same approach with the goal to deduce extensions of Theorem 4.1 to more than two variables as well as to Laurent polynomials P and Q of higher degree. This appears to quickly become considerably more intricate when approached in full generality. However, it is likely that one can obtain interesting results for special families of cases.

Likewise, it would be valuable to investigate general results in the spirit of Theorem 4.1 modulo prime powers p^r. We point the interested reader to Granville's engaging account [Gra97] for an extension of the Lucas congruences for binomial coefficients modulo p^r.

In a similar direction, it would be of interest to determine whether the sequences in Theorem 4.1 satisfy generalized versions of the Dwork congruences (5).

Acknowledgements

This project was initiated as part of the first author's master's thesis [Hen19], which includes Proposition 1.3 as well as Corollary 5.3, under the second author's guidance. The first author gratefully acknowledges summer support through a Sandra McLaurin Graduate Fellowship, and the second author is grateful for support through a Collaboration Grant (#514645) awarded by the Simons Foundation. The authors thank Eric Rowland for helpful comments and, in particular, for pointing out the notion of p-regular sequences [AS92].

References

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

[AS92] J.-P. Allouche and J. Shallit. The ring of k-regular sequences. *Theoretical Computer Science*, 98(2):163–197, May 1992.

[AZ06] G. Almkvist and W. Zudilin. Differential equations, mirror maps and zeta values. In *Mirror symmetry. V*, volume 38 of *AMS/IP Stud. Adv. Math.*, pages 481–515. Amer. Math. Soc., Providence, RI, 2006.

[Apé79] R. Apéry. Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque*, 61:11–13, 1979.

[BNSW11] J. M. Borwein, D. Nuyens, A. Straub, and J. Wan. Some arithmetic properties of short random walk integrals. *The Ramanujan Journal*, 26(1):109–132, 2011.

[Coo12] S. Cooper. Sporadic sequences, modular forms and new series for $1/\pi$. *The Ramanujan Journal*, 29(1–3):163–183, 2012.

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

[DS06] E. Deutsch and B. E. Sagan. Congruences for Catalan and Motzkin numbers and related sequences. *Journal of Number Theory*, 117(1):191–215, March 2006.

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

[Gor21] O. Gorodetsky. New representations for all sporadic Apéry-like sequences, with applications to congruences. *Experimental Mathematics*, 2021. DOI:10.1080/10586458.2021.1982080.

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

[Hen19] J. A. Henningsen. Sequences modulo primes and finite state automata. Master's thesis, University of South Alabama, 2019.

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

[Luc78] E. 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.

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

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

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

[Mes14] R. Meštrović. Lucas' theorem: its generalizations, extensions and applications (1878–2014). *Preprint*, September 2014. arXiv:1409.3820.

[Noe06] T. D. Noe. On the divisibility of generalized central trinomial coefficients. *Journal of Integer Sequences*, 9(2):06.2.7, 2006.

[Poo79] A. v. d. Poorten. A proof that Euler missed ... Apéry's proof of the irrationality of $\zeta(3)$. *Mathematical Intelligencer*, 1(4):195–203, 1979.

[RS09] L. B. Richmond and J. Shallit. Counting abelian squares. *The Electronic Journal of Combinatorics*, 16:#R72, 9 p., 2009.

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

[RZ14] E. Rowland and D. 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.

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

[Slo21] N. J. A. Sloane. The On-Line Encyclopedia of Integer Sequences, 2021. Published electronically at `http://oeis.org`.

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

[Zag09] D. B. Zagier. Integral solutions of Apéry-like recurrence equations. In *Groups and symmetries*, volume 47 of *CRM Proc. Lecture Notes*, pages 349–366. Amer. Math. Soc., Providence, RI, 2009.