Uniform Recurrence in the Motzkin Numbers and Related Sequences mod p

Nadav Kohen

Submitted: Jun 5, 2024; Accepted: Apr 8, 2025; Published: Jun 6, 2025

Abstract

Many famous integer sequences, including the Catalan numbers and the Motzkin numbers, can be expressed as the constant terms of the polynomials $P(x)^n Q(x)$ for some Laurent polynomial Q, and symmetric Laurent trinomial P. In this paper, we characterize the primes for which sequences of this form are uniformly recurrent modulo p. For all other primes, we show that the set of indices for which our sequences are congruent to 0 has density 1. This is accomplished by showing that the study of these sequences mod p can be reduced to the study of the generalized central trinomial coefficients, which are well-behaved mod p.

Mathematics Subject Classifications: 11B50, 68R15, 05A15, 11B85

1 Introduction

The Motzkin numbers (A001006 of [9]), M_n, count the number of lattice paths from the origin to $(n, 0)$, which do not go below the x-axis, with steps $U = (1, 1), L = (1, 0)$, and $D = (1, -1)$. See [6] for many other combinatorial settings in which the Motzkin numbers arise. Some work has been done to characterize M_n and similar sequences modulo various prime powers. For example, Deutsch and Sagan [5] characterized M_n mod 3. They also described all n such that $M_n \equiv 0 \pmod{p}$ for $p = 2, 4, 5$.

In recent years, much of this work has utilized Rowland and Zeilberger's finite automaton [11], which encodes the behavior of every sequence of the form ct $[P^n Q]$ mod p where ct stands for "constant term of," and P and Q are Laurent polynomials (possibly in multiple variables). Burns [4] has used these automata to study the asymptotic behavior of M_n mod small primes. And Rampersad and Shallit [10] have used these automata alongside the automatic theorem prover Walnut [8] (finite state automata have a decidable first-order theory) to re-prove Deutsch and Sagan's results, as well as showing that M_n mod 5 is uniformly recurrent (see Definition 1), and various other congruence properties of the Motzkin numbers, Catalan numbers, and central trinomial coefficients.

Department of Mathematics, Indiana University, Bloomington, Indiana, U.S.A. (nkohen@iu.edu).

 https://doi.org/10.37236/13089

The central trinomial coefficients (A002426 of [9]) are $T_n = \mathrm{ct}\,[(x^{-1}+1+x)^n]$. They are related to the Motzkin numbers since $M_n = \mathrm{ct}\,[(x^{-1}+1+x)^n(1-x^2)]$. From this, one can derive that $2M_n = 3T_n + 2T_{n+1} - T_{n+2}$ (see Section 4). In this paper, we call sequences of the form $a_n = \mathrm{ct}\,[(\alpha_{-1}x^{-1}+\alpha_0+\alpha_1 x)^n]$ *generalized central trinomial coefficients*.

In Problem 6 of [10], Rampersad and Shallit ask for a characterization of the primes, p, for which the Motzkin numbers mod p are uniformly recurrent. Based on Burns' results for small primes in [4], Rampersad and Shallit conjectured that the answer is the sequence of primes not dividing any central trinomial coefficient; these primes form the sequence A113305 of [9]. They also conjectured that for all other p, the Motzkin numbers mod p are 0 with density 1.

In this paper, we confirm these conjectures (Corollary 14). This is accomplished by showing that the set of primes, p for which every sequence that arises as an integral linear combination of generalized central trinomial coefficients is uniformly recurrent mod p, is the set of primes that do not divide any of the corresponding generalized central trinomial coefficients (Theorem 11). In particular, the Motzkin numbers can be described by such an integral linear combination. Furthermore, we confirm that for all other p, sequences of this form are 0 mod p with density 1.

In the case that p does divide a central trinomial coefficient, our approach is to utilize the fact that generalized central trinomial coefficients mod p are determined independently by the digits in their base-p expansions (Proposition 2). Thus, p must divide one of the first p coefficients and every index whose base-p expansion contains that digit. This forces the set of indices for which p divides that central trinomial coefficient to have density 1. Consequently, there are arbitrarily long runs of 0s, which inhibits uniform recurrence.

In the case that p does not divide any central trinomial coefficient, our approach is again to utilize Proposition 2 applied to integral linear combinations of the form $b_n = \sum_{i=0}^{h} a_{n+i}$, where $(a_n)_n$ is a sequence of generalized central trinomial coefficients. Specifically, the prefix of base-p digits that all of the indices $n, n+1, \ldots, n+h$ have in common can be factored out. And since individual central trinomial coefficients mod p recur within a constant bound (Lemma 7), we can force every word in our general sequence to recur by adding to this shared prefix, except for a few special cases treated separately.

Lastly, in Section 4 we show that sequences of the form $b_n = \mathrm{ct}\,[P(x)^n Q(x)]$, where P is a symmetric Laurent trinomial and Q is some arbitrary Laurent polynomial, can be written as combinations of $\mathrm{ct}\,[P(x)^{n+i}]$ for various i so that Theorem 11 applies to all sequences of the form $\mathrm{ct}\,[P(x)^n Q(x)]$. Lastly, we mention a situation in representation theory where such sequences arise and in that context Theorem 11 gives a surprising result.

1.1 Notation and Conventions

Throughout this paper, $P(x)$ denotes a Laurent trinomial of the form $\alpha_{-1}x^{-1}+\alpha_0+\alpha_1 x$ with $\alpha_i \in \mathbb{Z}$, while $Q(x)$ denotes an arbitrary Laurent polynomial with integer coefficients, and $\mathrm{ct}\,[Q(x)]$ denotes the constant term of $Q(x)$. For a fixed $P(x)$, we let a_n denote the nth term of the sequence $(\mathrm{ct}\,[P(x)^n])_{n\in\mathbb{N}}$.

If Σ is a set, Σ^* denotes the set of words (i.e., strings) of any length whose letters are from Σ (including the empty word). If n is a non-negative integer, and p is a prime then let $n_p \in \mathbb{F}_p^*$ be the word whose letters are the digits of n in base p. That is, if we let $n_p[i]$ denote the ith least significant digit in the base-p expansion of n so that $n = \sum_{i \in \mathbb{Z}_{\geqslant 0}} n_p[i] p^i$, then $n_p = (n_p\,[\text{length}(n_p) - 1]) \cdots (n_p[1])(n_p[0])$. Note that when working with strings, exponents denote repetition; for example, $(p-1)^k$ denotes a run of k letters that are all the letter $(p-1)$. Also, note that every statement made in this paper about n_p should also hold for $0^k n_p$ for every k.

This paper is primarily focused on showing when sequences mod primes are uniformly recurrent, which can be thought of as a weaker form of periodicity:

Definition 1. A sequence s_n is called *uniformly recurrent* if for every word in s_n (i.e., contiguous subsequence), $w = s_i s_{i+1} \cdots s_{i+\ell-1}$, there is a constant C_w such that every occurrence of w is followed by another occurrence of w at a distance of at most C_w. I.e., there is a $j \leqslant C_w$ such that $w = s_{i+j} s_{i+j+1} \cdots s_{i+j+\ell-1}$.

For background on uniform recurrence in automatic sequences, see Section 10.9 of [1].

2 Central Trinomial Coefficients

We begin by demonstrating why it is desirable to reduce to the study of generalized central trinomial coefficients when working mod p.

Proposition 2. *For every prime p and symmetric Laurent trinomial $P(x)$, the generalized central trinomial coefficients, $a_n = \operatorname{ct}[P(x)^n]$, satisfy $a_n \equiv \prod a_{n_p[i]} \pmod{p}$.*

Proof. We induct on the number of digits in n_p. Certainly if $n = n_p[0] < p$ then $a_n = a_{n_p[0]}$. Otherwise, if $n = qp + n_p[0]$, then

$$\begin{aligned}
a_n &= \operatorname{ct}\left[P(x)^{qp+n_p[0]}\right] \\
&\equiv \operatorname{ct}\left[P(x^p)^q P(x)^{n_p[0]}\right] \pmod{p} && (P(x)^p \equiv P(x^p) \pmod{p}) \\
&= \operatorname{ct}\left[P(x^p)^q\right] \operatorname{ct}\left[P(x)^{n_p[0]}\right] && (n_p[0] < p \text{ so there is no cancellation}) \\
&= \operatorname{ct}\left[P(x)^q\right] \operatorname{ct}\left[P(x)^{n_p[0]}\right] && \left(\operatorname{ct}\left[P(x^k)^n\right] = \operatorname{ct}\left[P(x)^n\right]\right) \\
&= a_q a_{n_p[0]} \\
&\equiv \prod a_{n_p[i]} \pmod{p} && (\text{by induction, since } q_p \text{ has fewer digits than } n_p).
\end{aligned}$$

Then the result follows. ∎

This is why the central trinomial coefficients, A002426 of [9], satisfy this Lucas congruence (see [7]) since they are defined by $T_n = \operatorname{ct}[(x^{-1} + 1 + x)^n]$. However, in the case that $\alpha_0 = 0$, one usually wants to discuss the sequence $\operatorname{ct}[(\alpha_{-1}x^{-1} + \alpha_1 x)^{2n}]$ since the odd powers all have 0 constant term. But this is no issue since $\operatorname{ct}[(\alpha_{-1}x^{-1} + \alpha_1 x)^{2n}]$ is equal to $\operatorname{ct}\left[(\alpha_{-1}^2 x^{-1} + 2\alpha_{-1}\alpha_1 + \alpha_1^2 x)^n\right]$ (for example, the central binomial coefficients, A000984 of [9], are $B_n = \operatorname{ct}[(x^{-1} + 2 + x)^n]$). This gives us,

Corollary 3. *If* $b_n = \mathrm{ct}\,[P(x)^{2n}] = a_{2n}$*, then* b_n *also satisfies the congruence*

$$b_n \equiv \prod b_{n_p[i]} \pmod p.$$

3 Combinations of Central Trinomial Coefficients

Here we characterize the primes, p, for which generalized central trinomial coefficients, $a_n = \mathrm{ct}\,[P(x)^n]$, are uniformly recurrent mod p. This was nearly accomplished in [10], but here we do away with the assumption that one of $\{a_0, a_1, \dots, a_{p-1}\}$ needs to be a primitive root. Additionally, the proof is extended to characterize the primes for which every integral linear combination of a_{n+i} is uniformly recurrent mod p, where the characterization is independent of the linear combination given.

In particular, weighted Motzkin sequences [12] (including the standard Motzkin sequence) can be written as integral linear combinations of generalized central trinomial coefficients, so the results in this section apply to these sequences.

We begin with the case where our sequences are not uniformly recurrent:

Example 4. The Motzkin numbers satisfy $2M_n = 3T_n + 2T_{n+1} - T_{n+2}$ where T_n is equal to $\mathrm{ct}\,[(x^{-1} + 1 + x)^n]$ (see Section 4 or [3]). If $p > 2$, then $M_{p,n} = 2^{-1}(3T_n + 2T_{n+1} - T_{n+2})$ gives us a sequence congruent to M_n mod p where 2^{-1} is the multiplicative inverse of 2 mod p.

Consider $p = 3$ so that $p \mid T_2 = 3$. Proposition 2 implies that $T_n \equiv 0$ whenever n_p contains a 2. This in turn implies that every time all three of $n_p, (n+1)_p, (n+2)_p$ contain a 2, then all three of $T_n, T_{n+1}, T_{n+2} \equiv 0$ and thus $M_n \equiv 0$. Thus, to find a run of 0s in M_n mod 3 of length at least 3^{k-1}, we can use the fact that for every integer, n, in the interval $[2(3)^k, 2(3)^k + 3^{k-1}]$, all three of $n, n+1, n+2$ have a 2 in their base 3 representations, so long as $k > 1$ (if $k = 1$ and $m = 2(3)^1 + 3^{1-1} = 2(3) + 1$, then $m + 2 = 3^2$).

Proposition 5. *If* p *is a prime dividing some element of* a_n*, and if* $b_n = \sum_{i=0}^{h} c_i a_{n+i}$ *where* $c_i \in \mathbb{Z}$*, then* $b_n \bmod p$ *has arbitrarily large runs of* 0*s. Thus,* $b_n \bmod p$ *is not uniformly recurrent. In particular, these statements hold for* $b_n = 1 \cdot a_n$*.*

Proof. Let $0 < z < p$ be an integer such that $a_z \equiv 0 \pmod p$. Because $b_n = \sum_{i=0}^{h} c_i a_{n+i} \equiv \sum_{i=0}^{h} \left(c_i \cdot \prod a_{(n+i)_p[j]}\right) \pmod p$ by Proposition 2, the prefix of base-p digits that all of the indices $n, \dots, n+h$ share, say a_{n_x} up to a_{n_y}, can be factored out of this sum so that we have

$$\begin{aligned}
b_n &\equiv \sum_{i=0}^{h}\left(c_i \cdot \prod a_{(n+i)_p[j]}\right)\\
&= \sum_{i=0}^{h}\left(c_i \cdot \prod_{j=x}^{y} a_{n_p[j]} \prod_{j<x} a_{(n+i)_p[j]}\right)\\
&= \prod_{j=x}^{y} a_{n_p[j]} \left(\sum_{i=0}^{h}\left(c_i \cdot \prod_{j<x} a_{(n+i)_p[j]}\right)\right).
\end{aligned}$$

In particular, we have that if $n_p[j] = z$ for some $x \leqslant j \leqslant y$, then $b_n \equiv 0 \pmod p$. Therefore, for sufficiently large integers k (relative to the length of h_p), $z \cdot p^k$ marks the beginning of a run of 0s mod p of length at least p^{k-1} since $\left(z \cdot p^k\right)_p = z0^k$ (i.e., z followed by k 0s). And p^{k-1} can be made arbitrarily large. □

Proposition 6. *If p is a prime dividing some element of a_n, and if $b_n = \sum_{i=0}^{h} c_i a_{n+i}$ where $c_i \in \mathbb{Z}$, then 0 has density 1 in the sequence $b_n \bmod p$.*

Proof. As mentioned in the proof of Proposition 5, if some digit is z (such that $p \mid a_z$) in a shared prefix of a run of indices, n through $n+h$, then $b_n \equiv 0 \pmod p$. If β is the length of h_p, then consider the first p^k terms of our sequence ($n = 0, \dots, p^k - 1$). For $k > \beta$, if any of the first $(k-\beta)$ digits of an index n_p are z, then that z must be part of the shared prefix (i.e., every string $n_p, \dots, (n+h)_p$ have a z in that position) and so $b_n \equiv 0$. So there are at least $p^k - (p-1)^{k-\beta}p^\beta$ of the first p^k terms of b_n that are divisible by p (since there are $p-1$ choices for the first $k-\beta$ digits of n_p that allow non-zero b_n), and so the proportion is at least $\frac{p^k-(p-1)^{k-\beta}p^\beta}{p^k} = 1 - \frac{p^\beta}{(p-1)^\beta}\left(\frac{p-1}{p}\right)^k \to 1$ as $k \to \infty$. □

This completes the characterization of what happens when $p \mid a_n$ for some a_n. We now turn to the case where $p \nmid a_n$ for all n, in which case our sequences are uniformly recurrent. This result mostly boils down to using the fact that $a_n \bmod p$ has uniform recurrence for words of length 1:

Lemma 7. *If $p \nmid a_n$ for all n, then for every $n \in \mathbb{Z}_{\geqslant 0}$, there is an $n' \in \mathbb{Z}_{\geqslant 0}$ such that $n' > n$, $n' - n < p^{p(p-1)+p+1}$, and $a_n \equiv a_{n'} \pmod p$.*

Proof. Given n, write it as a word in $\{0, 1, \dots, p-1\}^*$ via its base-p expansion

$$n_p = n^*(n_p[p^{p-1}]) \cdots (n_p[1])(n_p[0]),$$

where the leading $n_p[i]$ may be 0 and $n^* \in \{0, 1, \dots, p-1\}^*$ may be the empty word. We find n' by altering only this suffix (or slightly more) to achieve the bound. We describe n' in an exhaustive set of cases:
Case 1: $\exists i > j$ such that $n_p[i] < n_p[j]$.

Since the value of $a_n \bmod p$ is independent of the order of the digits in n_p by Proposition 2, we can let n' be the result of switching the ith and jth (least significant) digits of n.

Case 2: The digits $n_p[p^{p-1}]$ through $n_p[0]$ are in descending order.

By the pigeonhole principle there is some i such that

$$n_p[i] = n_p[i-1] = \cdots = n_p[i-(p-2)].$$

Because $p \nmid a_{n_p[i]}$, we can apply Fermat's little theorem to see that the contribution of these digits is $a_{n_p[i]}^{p-1} \equiv 1 \pmod{p}$.

Case 2a: $\exists i < p-1$ with $n_p[i] = n_p[i-1] = \cdots = n_p[i-(p-2)]$.

We can let n' be the result of replacing digits i through $i-(p-2)$ in n with the letter $(n_p[i]+1)$, which results in the same contribution to the product of Proposition 2 of $a_{n_p[i]+1}^{p-1} \equiv 1 \pmod{p}$.

Case 2b: n_p is of the form $n^{**}(n_p[k+|\gamma|])(p-1)^k\gamma$ where $k > p$, $\gamma \in \{0,1,\dots,p-2\}^*$, $|\gamma| < p^{p-1}-p$, and $n_p[k+|\gamma|] \neq p-1$ is the least significant non-$(p-1)$ digit in n^*.

If $k = q(p-1)+r$ with $r < p-1$, we can let n' correspond to the word

$$(n')_p = n^{**}(n_p[k+|\gamma|]+1)0^{(q-1)(p-1)}(n_p[k+|\gamma|])(n_p[k+|\gamma|]+1)^{p-2}(p-1)^r\gamma.$$

Again using Proposition 2, that $p \nmid n_p[i]$ for all i, and Fermat's little theorem, it is clear that $a_n \equiv a_{n'} \pmod{p}$. ☐

Example 8. To illustrate this last case, let $p=5$ and consider the sequence $a_n = T_n = \mathrm{ct}\left[(x^{-1}+1+x)^n\right]$. Let $n_p = 12324^{678}333222111000$ so that $n^{**} = 123$, $\gamma = 333222111000$, $k = 678$, $q = 169$, $r = 2$, and $n_p[k+|\gamma|] = 2$. Then $(n')_p = 12330^{672}23^34^2333222111000$. Both n and n' have the same number of each possible digit mod $p-1=4$ so that by Proposition 2 and Fermat's little theorem, T_n and $T_{n'}$ are congruent.

We now give examples to motivate the approach in the proof of our main theorem.

Example 9. Let $p=5$, $a_n = T_n$ and $b_n = M_{p,n} = 2^{-1}(3a_n + 2a_{n+1} - a_{n+2})$ as in Example 4. Consider $n = 75156245$ so that $n_p = 123214444443$, $(n+1)_p = 123214444444$, and $(n+2)_p = 123220000000$. One method for constructing an $n' > n$ such that $b_n \equiv b_{n'}$ is to use the fact that each of a_n, a_{n+1}, and a_{n+2} share a factor of $a_1a_2a_3a_2 = a_{192}$ (because $192_p = 1232$) from the shared prefix of these three indices. Thus we can use Lemma 7 to add some value to this shared prefix. In this case, it just so happens that $a_{192} \equiv 3 \equiv a_{199}$ so we can let $n' = n + 7(5)^8$. All three pairs $(n,n'), (n+1,n'+1)$, and $(n+2,n'+2)$ have congruent numbers of each possible digit mod $p-1$, so that $b_n \equiv b_{n'}$. However, we have actually accomplished more than this: if we let $\Delta = n'-n$ then every index from $m_p = 123200000000$ to 123244444444 satisfies $b_m \equiv b_{m+\Delta}$.

Example 10. Again let $p=5, a_n = T_n, b_n = M_{p,n}$ and $n = 75156245$. An alternative method for constructing an $n' > n$ such that $b_n \equiv b_{n'}$ is to use Fermat's little theorem to replace $p-1$ of the 4s, and to use those positions to undo the effect of incrementing the first non-4 digit. We turn $n_p = (1232)1(4444)443$ into $(n')_p = (1232)2(2221)443$. Just as in the previous example, not only is $b_n \equiv b_{n'}$ but if $\Delta = n'-n$, then $b_m \equiv b_{m+\Delta}$ for all m from $m_p = 123214444000$ through 123220000443.

Note that one can always use the method of Example 9 to cause a recurrence in b_n without requiring any structure on n. However, there is no general bound on Δ when this method is used. On the other hand, the method of Example 10 requires access to $p-1$ consecutive copies of the digit $(p-1)$, and bounds Δ relative to the first such occurrence.

Theorem 11. *If $a_n = \mathrm{ct}\,[P(x)^n]$ where $P(x) = \alpha_{-1}x^{-1}+\alpha_0+\alpha_1 x$, and if $b_n = \sum_{i=0}^{h} c_i a_{n+i}$ where $c_i \in \mathbb{Z}$, then $(b_n)_{n\in\mathbb{N}}$ is uniformly recurrent mod p if and only if p does not divide any a_n (which can be checked for $n < p$).*

Proof. One direction is Proposition 5, so we need only show that if $p \nmid a_n$ for all n (so that Lemma 7 applies), then b_n is uniformly recurrent mod p.

Given a word, $w = (b_i \bmod p)(b_{i+1} \bmod p)\cdots(b_{i+\ell-1} \bmod p)$ of length ℓ, we wish to bound the next occurrence of w in $(b_n)_{n\in\mathbb{N}}$, and the bound must be independent of i.

First, a proof sketch: Let p^s be the largest power of p that has a multiple in the open interval $(i-1, i+h+\ell)$. Note that this interval gives us the indices that appear if we expand the digits of w into sums of elements of the sequence $(a_n)_{n\in\mathbb{N}}$. If p^s is small relative to h (Case 1), or small relative to ℓ (Case 2a), then since our bound need not be independent of h or ℓ, we can utilize the method demonstrated in Example 9 of using Lemma 7 to add to a shared prefix of the base-p representations of the indices in the open interval $(i-1, i+h+\ell)$ to find a recurrence of w. Otherwise, if p^s is large relative to both h and ℓ (Case 2b), then we are assured to have the conditions for which it is possible to use the method demonstrated in Example 10 of using Fermat's little theorem to find a recurrence.

Let β be the length of h_p. Let $\alpha \geqslant 1$ be the largest integer such that

$$p^{(\alpha-1)(p-1)+\beta} - p^{\beta} \leqslant \ell$$

(note that $\ell < p^{\alpha(p-1)+\beta} - p^{\beta}$). Let $k = s-\beta$ and write $k = q(p-1)+r$ where q and r are non-negative integers and $r < p-1$. Let C be a fixed bound on the recurrence of every a_n, which is guaranteed to exist (and can be less than $p^{p^{p-1}+p+1}$) by Lemma 7. We prove that $(b_n)_{n\in\mathbb{N}}$ is uniformly recurrent mod p by showing that w recurs within a difference of index of at most $C \cdot p^{3p+\alpha+\beta}\ell$ (independently of i).

Case 1: $s < \beta + p$.

Clearly, $p^s < p^{3p+\beta}\ell$. In the following case, we prove the same bound and then justify that the result follows for both Cases 1 and 2a in the subsequent conclusion.

Case 2a: $s \geqslant \beta + p$ and $q \leqslant \alpha$.

As in Case 1, we also have the same inequality,

$$\begin{aligned}
p^s &= p^{k+\beta} \\
&= p^{(q-1)(p-1)+\beta} p^{p-1+r} && (k = q(p-1)+r) \\
&\leqslant p^{p-1+r}(\ell + p^\beta) && (q \leqslant \alpha \text{ and } p^{(\alpha-1)(p-1)+\beta} \leqslant \ell + p^\beta) \\
&\leqslant p^{2p}(1+p^\beta)\ell && (r < p \text{ and } \ell + p^\beta \leqslant \ell + \ell p^\beta) \\
&\leqslant p^{3p+\beta}\ell. && (1 + p^\beta \leqslant p^{p+\beta}).
\end{aligned}$$

Conclusion for Cases 1 and 2a:

The base-p representations of all indices in the open interval $(i-1, i+h+\ell)$ share a prefix above the s'th least significant digit by our choice of s. That is, every integer in this interval has a base-p representation of the form $n^* n^{**}$ where $n^* \in \{0, \ldots, p-1\}^*$ and $n^{**} \in \{0, \ldots, p-1\}^s$ for a fixed n^* and variable n^{**}. Thus, adding Δp^s to all indices simply results in the addition of Δ to their shared prefix, n^*. Therefore, by Lemma 7, we can pick $\Delta < C$ such that $a_{n^*} \equiv a_{n^*+\Delta}$ implying, by Proposition 2, that $a_{n^* n^{**}} \equiv a_{(n^*+\Delta)n^{**}} = a_{n^* n^{**} + \Delta p^s}$ for all n^{**} and so w recurs beginning at index $i + \Delta p^s$. Lastly, since in both cases we have that $p^s \leqslant p^{3p+\beta}\ell$, we can conclude that $\Delta p^s \leqslant C \cdot p^{3p+\alpha+\beta}\ell$.

Case 2b: $s \geqslant \beta + p$ and $q > \alpha$.

Let n be the first index such that $n + h$ is a multiple of $p^s = p^{k+\beta}$. Then

$$n_p = n^*(m)(p-1)^k \gamma$$

where $n^* \in \{0, \ldots, p-1\}^*$, $m \in \{0, \ldots, p-2\}$, and $\gamma \in \{0, \ldots, p-1\}^\beta$. Let Δ be the integer such that $\Delta_p = (m+1)^{p-1} 0^{\alpha(p-1)+r+\beta}$. Note that $\Delta < p^{(2+\alpha)p+\beta}$. We begin by inspecting

$$(n+\Delta)_p = n^*(m+1)0^{(q-\alpha-1)(p-1)}(m+1)^{p-2}(m)(p-1)^{\alpha(p-1)+r}\gamma.$$

First note that $b_n \equiv b_{n+\Delta} \pmod p$ by Fermat's little theorem. Next note that because $\ell < p^{\alpha(p-1)+\beta} - p^\beta$ we have that $i+\Delta, i+\Delta+1, \ldots, n+\Delta+h-1$ all have the shared prefix

$$n^*(m+1)0^{(q-\alpha-1)(p-1)}(m+1)^{p-2}m$$

whose contribution is the same as $n^* m$; meanwhile all of $n+\Delta+h, \ldots, i+\Delta+\ell-1$ have the shared prefix

$$n^*(m+1)0^{(q-\alpha-1)(p-1)}(m+1)^{p-1}$$

whose contribution is the same as $n^*(m+1)$. Therefore, $a_{i+j} \equiv a_{i+\Delta+j} \pmod p$ for all $0 \leqslant j < \ell$, and thus w recurs beginning at index $i + \Delta$. Lastly,

$$\Delta \leqslant p^{(2+\alpha)p+\beta} = p^{(\alpha-1)(p-1)+\beta} p^{3p+\alpha-1} \leqslant p^{3p+\alpha-1}(\ell + p^\beta) \leqslant p^{3p+\alpha+\beta}\ell \leqslant C \cdot p^{3p+\alpha+\beta}\ell,$$

as desired. □

Remark 12. Because p^α is bounded by some constant times $\ell^{\frac{1}{p-1}}$, our recurrence bound is a constant times $\ell^{\frac{p}{p-1}}$. This bound has a much larger constant factor than the one observed in Theorem 5 of [10] (200ℓ for the Motzkin numbers mod 5). Additionally, the bound here grows faster than $O(\ell)$ as is observed in Theorem 5 of [10]. The author suspects that in the case that one of the first p elements of a_n is a primitive root, then there is an alternative argument that uses inverses in place of Fermat's little theorem to achieve an $O(\ell)$ bound.

Using our main result, we can now draw as corollaries a refinement of Theorem 10 from [10] as well as validate the conjecture of Problem 6 from [10] proving that Burns' observations in [4] hold in general.

Corollary 13. *The central trinomial coefficients mod p are uniformly recurrent if and only if p does not divide any of the central trinomial coefficients (which can be checked for $n < p$). Furthermore, if p does divide a central trinomial coefficient, then 0 has density 1 in the central trinomial coefficients mod p.*

Corollary 14. *The Motzkin numbers are uniformly recurrent mod p if and only if p does not divide any central trinomial coefficients. Furthermore, if p does divide a central trinomial coefficient, then 0 has density 1 in the Motzkin numbers mod p.*

Proof. The Motzkin numbers satisfy $2M_n = 3T_n + 2T_{n+1} - T_{n+2}$, where T_n is equal to $\mathrm{ct}\,[(x^{-1}+1+x)^n]$ (see the next section or [3]), so the theorem applies for all primes $p > 2$ because $M_n \equiv M_{p,n} \pmod p$ and $M_{p,n} = 2^{-1}(3T_n + 2T_{n+1} - T_{n+2})$. For $p = 2$, one can prove uniform recurrence directly from the automaton of Figure 1 in [10]. Ignoring the least significant digit, the figure shows that the value of $M_n \bmod 2$ is determined by the position of the first 0 in $(n)_2$ (from the right). So if $w = (M_n \bmod 2)(M_{n+1} \bmod 2) \cdots (M_{n+\ell-1} \bmod 2)$, then we can let Δ be one of $2^{\lfloor \log_2 \ell \rfloor + 1}$ or $2^{\lfloor \log_2 \ell \rfloor + 2}$ and at least one of these yields $w = (M_{n+\Delta} \bmod 2) \cdots (M_{n+\Delta+\ell-1} \bmod 2)$, as desired.

Lastly, Proposition 6 completes the corollary. □

The fact that the Motzkin numbers have an identity in terms of the central trinomial coefficients is no coincidence, and we detail this connection in the following section.

4 A Family of Applicable Sequences

We now generalize our results for the Motzkin numbers slightly to sequences of the form $\mathrm{ct}\,[P(x)^n Q(x)]$ where P is of the (symmetric) form $\alpha_1 x^{-1} + \alpha_0 + \alpha_1 x$ and Q is some arbitrary Laurent polynomial. For example, $P(x) = x^{-1} + 1 + x$ with $Q(x) = 1 - x^2$ gives us the Motzkin numbers (in fact, any symmetric P with this $Q(x)$ yields a weighted Motzkin sequence [12]), whereas the same P with $Q(x) = 1 - x$ gives the Riordan numbers, A005043 of [9], and $P(x) = x^{-1} + 2 + x^2$ with $Q(x) = 1 - x$ gives the Catalan numbers, A000108 of [9].

Proposition 15. *If $a_n = \mathrm{ct}\,[P(x)^n]$ where $P(x) = \alpha_1 x^{-1} + \alpha_0 + \alpha_1 x$ and $Q(x)$ is some arbitrary Laurent polynomial, then for $p > 2$, $b_n = \mathrm{ct}\,[P(x)^n Q(x)]$ is uniformly recurrent mod p if and only if p does not divide any a_n (which can be checked for $n < p$).*

Proof. In view of Theorem 11, it suffices to find an integral linear combination of the a_{n+i} that yields a sequence congruent to b_n mod p.

Let $a_{n,i} = \mathrm{ct}\,[P(x)^n x^i]$, which is the same as the coefficient of x^i (or x^{-i}) in $P(x)^n$ (so $a_{n,0} = a_n$). Notice that $a_{n+i,0} = \sum_{j=-i}^{i} a_{i,j} \cdot a_{n,j} = a_{i,0} \cdot a_{n,0} + \sum_{j=1}^{i} 2a_{i,j} \cdot a_{n,j}$ (see Figure 1 to see where this identity comes from). This along with the fact that $a_{i,i} = \alpha_1^i$ yields $2\alpha_1^i \cdot a_{n,i} = a_{n+i,0} - a_{i,0} \cdot a_{n,0} - \sum_{j=1}^{i-1} 2a_{i,j} \cdot a_{n,j}$. Finally, induction applied to $a_{n,j}$ with $j < i$ using this equality shows that if $p \nmid \alpha_1$, then $a_{n,i}$ can be written as linear combination of $a_{n,0}, a_{n+1,0}, \dots, a_{n+i,0}$ over $\mathbb{F}_p$ (since 2 and α_1 are units). In fact, if $\alpha_1 = 1$ then we even get that $2 \cdot a_{n,i}$ can be written outright as an integral linear combination in this way. For example, if $P(x) = x^{-1} + 1 + x$ and $Q(x) = 1 - x^2$, we get an identity for the Motzkin numbers in terms of the central trinomial coefficients by finding an identity for $a_{n,2}$ (and $a_{n,0}$) in terms of central coefficients (see the example below).

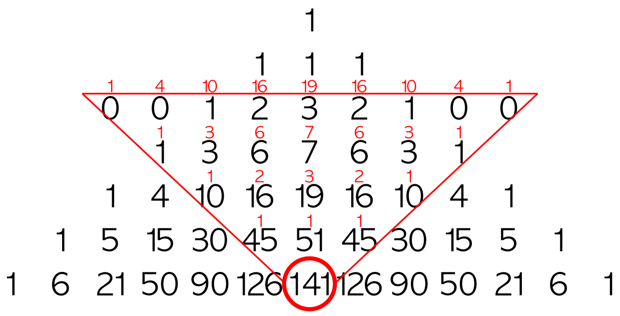

Figure 1: A demonstration of why $a_{n+i,0} = \sum_{j=-i}^{i} a_{i,j} \cdot a_{n,j}$ when $\alpha_0 = \alpha_1 = 1$. The small red numbers count the number of contributions of each number in a row to the circled 141.

Thus, in the case that $p \nmid \alpha_1$, if $Q(x) = \sum_{j \in \mathbb{Z}} c_j x^j$ then $b_n = \mathrm{ct}\,[P(x)^n Q(x)]$ is equal to $\sum_{j \in \mathbb{Z}} c_j a_{n,-j}$, which is congruent mod p to a linear combination of a_{n+i}'s (with $0 \leqslant i \leqslant \max(\deg Q(x), \deg Q(x^{-1}))$), and so Theorem 11 applies.

On the other hand, if $\alpha_1 \equiv 0 \pmod{p}$, then we simply get

$$b_n \equiv \mathrm{ct}\,[\alpha_0^n Q(x)] = \alpha_0^n \cdot \mathrm{ct}\,[Q(x)] \pmod{p},$$

which is periodic (and thus uniformly recurrent).

In either case, for every $p > 2$, b_n is uniformly recurrent. □

Example 16. Let's show where the identity, $2M_n = 3T_n + 2T_{n+1} - T_{n+2}$, that we have been using to apply our results to the Motzkin numbers comes from. First note that $M_n = \mathrm{ct}\,[(x^{-1}+1+x)^n(1-x^2)] = \mathrm{ct}\,[(x^{-1}+1+x)^n] - \mathrm{ct}\,[(x^{-1}+1+x)^n x^2] = a_{n,0} - a_{n,2}$. Thus, if we let $T_n = \mathrm{ct}\,[(x^{-1}+1+x)^n] = a_{n,0}$, $A_n = \mathrm{ct}\,[(x^{-1}+1+x)^n x] = a_{n,1}$ and $B_n = \mathrm{ct}\,[(x^{-1}+1+x)^n x^2] = a_{n,2}$, then we can use that $T_{n+2} = 3T_n + 4A_n + 2B_n$ and $T_{n+1} = T_n + 2A_n$ (see Figure 1 for justification) to see that

$$3T_n + 2T_{n+1} - T_{n+2} = 2(T_n - B_n) = 2M_n.$$

4.1 Application to Representation Theory

Let $\mathrm{SU}(2,\mathbb{C})$ denote the Lie group of 2 by 2 unitary matrices with complex entries and determinant 1. See [2] for background on the representations of $\mathrm{SU}(2,\mathbb{C})$. If we let V_k denote the k-dimensional irreducible representation of $\mathrm{SU}(2,\mathbb{C})$, then the number of irreducible components of dimension d in $(V_1^{m_1} \oplus V_2^{m_2})^{\otimes n}$ yields a sequence for every d, m_1, and m_2 in $\mathbb{Z}_{\geqslant 0}$. Call this sequence b_n^{d,m_1,m_2}. Because $V_1^{m_1} \oplus V_2^{m_2}$ has character $m_2 x^{-1} + m_1 + m_2 x$, our sequence happens to have the form $b_n^{d,m_1,m_2} = \mathrm{ct}\,[P(x)^n Q(x)]$ where $P(x) = m_2 x^{-1} + m_1 + m_2 x$ and $Q(x) = x^{d-1} - x^{d-3}$. Well-known examples include $b_n^{1,1,1}$, which are the Motzkin numbers, and $b_n^{1,2,1}$, which are the Catalan numbers. Since these sequences have such a description by polynomials, if we reduce modulo a prime, Proposition 15 applies to all $b_n^{d,m_1,m_2} \bmod p$. Furthermore, Proposition 15 shows that the uniform recurrence of b_n is independent of $Q(x)$; therefore, for a fixed representation, $V_1^{m_1} \oplus V_2^{m_2}$, all of the sequences in the family $\{b_n^{d,m_1,m_2} \bmod p\}_{d>0}$ are either simultaneously uniformly recurrent or else simultaneously congruent to 0 with density 1 (by Proposition 6) for each prime, p.

Acknowledgements

The author would like to thank the referee for their invaluable and detailed review of this paper.

References

[1] J.-P. Allouche and J. Shallit. *Automatic Sequences: Theory, Applications, Generalizations.* Cambridge University Press, 2003.

[2] M. Artin. *Algebra.* Pearson Education, 2011.

[3] E. Barcucci, R. Pinzani, and R. Sprugnoli. The Motzkin family. *Pure Mathematics and Applications. Series A*, 2(3-4):249–279, 1992.

[4] R. Burns. Structure and asymptotics for Motzkin numbers modulo small primes using automata, 2016. Preprint arXiv:1612.08146.

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

[6] R. Donaghey and L. W. Shapiro. Motzkin numbers. *Journal of Combinatorial Theory, Series A*, 23(3):291–301, 1977.

[7] J. A. Henningsen and A. Straub. Generalized Lucas congruences and linear p-schemes. *Advances in Applied Mathematics*, 141:Paper No. 102409, 20, 2022.

[8] H. Mousavi. Automatic theorem proving in Walnut, 2021. Preprint arXiv:1603.06017.

[9] OEIS Foundation Inc. (2024). The On-Line Encyclopedia of Integer Sequences. Published electronically at https://oeis.org.

[10] N. Rampersad and J. Shallit. Congruence properties of combinatorial sequences via Walnut and the Rowland-Yassawi-Zeilberger automaton. *Electronic Journal of Combinatorics*, 29(3):#P3.36, 2022.

[11] E. S. Rowland and D. Zeilberger. A case study in meta-automation: automatic generation of congruence automata for combinatorial sequences. *Journal of Difference Equations and Applications*, 20:973–988, 2013.

[12] W.-J. Woan. A recursive relation for weighted Motzkin sequences. *Journal of Integer Sequences*, 8(1):Article 05.1.6, 2005.