MOTZKIN NUMBERS AND RELATED SEQUENCES MODULO POWERS OF 2

C. KRATTENTHALER† AND T. W. MÜLLER*

Abstract. We show that the generating function $\sum_{n\ge0} M_n\,z^n$ for Motzkin numbers M_n, when coefficients are reduced modulo a given power of 2, can be expressed as a polynomial in the basic series $\sum_{e\ge0} z^{4^e}/(1-z^{2\cdot4^e})$ with coefficients being Laurent polynomials in z and $1-z$. We use this result to determine M_n modulo 8 in terms of the binary digits of n, thus improving, respectively complementing earlier results by Eu, Liu and Yeh [*Europ. J. Combin.* **29** (2008), 1449–1466] and by Rowland and Yassawi [*J. Théorie Nombres Bordeaux* **27** (2015), 245–288]. Analogous results are also shown to hold for related combinatorial sequences, namely for the Motzkin prefix numbers, Riordan numbers, central trinomial coefficients, and for the sequence of hex tree numbers.

1. Introduction

The *Motzkin numbers* M_n may be defined by (cf. [11, Ex. 6.37])

$$\sum_{n\ge0} M_n\,z^n=\frac{1-z-\sqrt{1-2z-3z^2}}{2z^2}. \tag{1.1}$$

They have numerous combinatorial interpretations, see [11, Ex. 6.38]. The most basic one says that M_n equals the number of lattice paths from $(0,0)$ to $(n,0)$ consisting of steps taken from the set $\{(1,0),(1,1),(1,-1)\}$ never running below the x-axis.

Deutsch and Sagan [3, Theorem 3.1] determined the parity of M_n. Furthermore, they conjectured [3, Conj. 5.5] (a conjecture which is in part also due to Amdeberhan) that M_n is divisible by 4 if, and only if,

$$n=(4i+1)4^{j+1}-1 \quad\text{or}\quad n=(4i+3)4^{j+1}-2,$$

for some non-negative integers i and j. This conjecture prompted Eu, Liu and Yeh [4] to embark on a more systematic study of Motzkin numbers modulo 4 and 8. They approached this problem by carefully analysing a binomial sum representation for M_n modulo 4 and 8. They succeeded in establishing the above conjecture of Amdeberhan, Deutsch and Sagan. Moreover, they were able to characterise the even congruence classes of M_n modulo 8; see [4, Theorem 5.5] and Corollary 12 at the end of the present paper. One outcome of this characterisation is that M_n is never divisible by 8, thus proving another conjecture of Deutsch and Sagan [3, Conj. 5.5].

2000 *Mathematics Subject Classification.* Primary 05A15; Secondary 05E99 11A07 68W30.

Key words and phrases. Motzkin numbers, Motzkin prefix numbers, Riordan numbers, hex tree numbers, central trinomial coefficients, congruences, Lambert series.

†Research partially supported by the Austrian Science Foundation FWF, grants Z130-N13 and S50-N15, the latter in the framework of the Special Research Program “Algorithmic and Enumerative Combinatorics”

*Research supported by Lise Meitner Grant M1661-N25 of the Austrian Science Foundation FWF.

As part of a general theory of diagonals of rational functions, Rowland and Yassawi [10, Sec. 3.2] are able to approach the problem of determination of Motzkin numbers modulo powers of 2 from a completely different point of view. Their general theory (and algorithms) produce automata which output the congruence class of diagonal coefficients of a given rational function modulo a given power of a prime number. Since the Motzkin numbers M_n can be represented as the diagonal coefficients of a certain rational function, this theory applies, and consequently, for any prime power p^α, an automaton can be produced which outputs the congruence class of M_n modulo p^α. Rowland and Yassawi present the automaton for the determination of M_n modulo 8 in [10, Fig. 4].

The main purpose of this paper is to present yet another approach to the determination of Motzkin numbers M_n modulo powers of 2, namely by the use of generating functions. Our approach is in line with our earlier studies [7, 8, 9], in which we developed a generating function method for determining the mod-p^α behaviour of sequences whose generating functions satisfy algebraic differential equations. Application of this method to a concrete class of problems starts with the choice of a (usually transcendental) basic series. The goal then is to show that the generating function of the sequence that we are interested in can be expressed as a polynomial in this basic series when the terms of the sequence are reduced modulo p^α. Once this is achieved, one tries to extract a characterisation of the congruence behaviour of the sequence under consideration modulo p^α from this polynomial representation of the generating function. However, the details — such as the choice of basic series, or the extraction of coefficients from its powers — have to be adjusted for each individual class of applications.

Here, we choose the series $\Omega(z)$ defined by

$$\Omega(z) = \sum_{e\ge0}\sum_{f\ge0} z^{4^e(2f+1)} = \sum_{e\ge0} \frac{z^{4^e}}{1-z^{2\cdot 4^e}} \tag{1.2}$$

as basic series. In plain words, the series $\Omega(z)$ is the sum of all monomials z^m, where m runs through all positive integers with an even number of zeroes to the far right of their binary representation.

Our first main result, Theorem 6, states that the generating function $\sum_{n\ge0} M_n\, z^n$ for the Motzkin numbers, when coefficients are reduced modulo a given power of 2, can be expressed as a polynomial in $\Omega(z^4)$ with coefficients that are Laurent polynomials in z and $1-z$.

Theorem 6 may be implemented, so that these polynomial expressions can be found automatically modulo any given power of 2. Thus, our result in principle opens up the possibility of deriving congruences modulo arbitrary 2-powers for the sequence of Motzkin numbers, provided one is able to systematically extract coefficients from powers of the series $\Omega(z^4)$. However, for exponents greater than 3, this task turns out to be difficult and rather involved, though possible in principle. For this reason, we proceed differently. We use our algorithm to obtain a congruence modulo 16 exhibiting the generating function of the Motzkin numbers as a polynomial of degree 7 in $\Omega(z^4)$, and then drastically simplify the resulting expression modulo $2^3 = 8$ at the expense of introducing a certain "error-series" $E(z)$. The advantage is that, in this step, the degree of $\Omega(z^4)$ drops from 7 to 1. Extracting coefficients of powers of z from the resulting expression, we are then able to go beyond the result [4, Theorem 5.5] of Eu, Liu and

Yeh by providing a formula for the congruence class of M_n also in the case that M_n is odd; see Theorem 11. As demonstrated in Corollary 13, this result may conveniently be used to precisely characterise those n for which M_n lies in a specified congruence class modulo 8.

In a sense, our generating function method and the automaton method of [10] are complementary to each other. It is through our method that we were led to the explicit characterisation of the congruence behaviour of Motzkin numbers modulo 8 in Theorem 11 and Corollary 13, and to the explicit characterisations of the congruence behaviour modulo 8 of Motzkin prefix numbers, of Riordan numbers, of hex tree numbers, and of central trinomial coefficients in Theorems 14–17, together with proofs in each case. It seems hard to *extract* these results from the automata that one obtains by the theory in [10]. On the other hand, as pointed out by a referee, once these results are *known*, they can be *verified* using the theory of automata on the basis of the automata that one finds by means of the automaton theory of [10], since the functions $s_2(n)$, $s_2^2(n)$, $e_2(n)$, n_4, n_{K+1} that appear in these results are 2-regular sequences.

Our paper is organised as follows. In the next section, we derive some properties of our basic series $\Omega(z)$ defined in (1.2) that we shall need in the sequel. Section 3 outlines our generating function approach based on the series $\Omega(z)$. Subsequently, in Section 4, we apply this method to the generating function $M(z) = \sum_{n\ge0} M_n\, z^n$ for Motzkin numbers. This section contains our first main result, Theorem 6, stating that $M(z)$, when coefficients are reduced modulo a given power of 2, can be expressed as a polynomial in $\Omega(z)$. In Section 5, we specialise this result to the modulus $2^4 = 16$, see (5.1). This expression is then reduced modulo 8 and further simplified, at the cost of introducing an "error series" $E(z)$, defined in (5.3). The final expression for the mod-8 reduction of $M(z)$ is presented in (5.4). The remaining task is to extract the coefficient of z^n from the right-hand side of (5.4). In order to accomplish this, we provide several auxiliary lemmas in Section 6. In Section 7, making use of these lemmas, we are then able to provide explicit formulae for the congruence class of M_n modulo 8 in terms of the binary digits of n. This leads to our second main result which is presented in Theorem 11. In Corollary 13, we demonstrate by means of an example how to characterise those n for which M_n lies in a given congruence class modulo 8. Our final section then collects together results analogous to Theorem 11 for sequences related to Motzkin numbers, namely for the Motzkin prefix numbers, Riordan numbers, hex tree numbers, and the central trinomial coefficients; see Theorems 14–17. These results generalise earlier ones of Deutsch and Sagan [3] from modulus 2 to modulus 8.

Note. This paper is accompanied by a *Mathematica* file and a *Mathematica* notebook so that an interested reader is able to redo (most of) the computations that are presented in this article. File and notebook are available at the article's website `http://www.mat.univie.ac.at/~kratt/artikel/2motzkin.html`.

2. The power series $\Omega(z)$

Here we consider the formal power series $\Omega(z)$ defined in (1.2). This series is the principal character in the method for determining congruences of recursive sequences modulo 2-powers that we describe in Section 3. This series is transcendental over $\mathbb{Z}[z]$.[1]

[1] The quickest argument uses coefficient asymptotics for algebraic functions. The coefficients of $\Omega(z)$ do not approach any limit. Since these coefficients are 0 or 1, there is no asymptotic formula for them.

However, if the coefficients of $\Omega(z)$ are considered modulo a 2-power 2^γ, then $\Omega(z)$ obeys a polynomial relation with coefficients that are Laurent polynomials in z and $1-z$. This is shown in Proposition 1 below. In the second part of this section, we show that the derivative of $\Omega(z)$, when coefficients are reduced modulo a given 2-power, can be expressed as a polynomial in z and $(1-z)^{-1}$. This is one of the crucial facts which make the method described in Section 3 work.

Here and in the sequel, given integral power series (or Laurent series) $f(z)$ and $g(z)$, we write

$$f(z) = g(z) \text{ modulo } 2^\gamma$$

to mean that the coefficients of z^i in $f(z)$ and $g(z)$ agree modulo 2^γ for all i.

Proposition 1. *We have*

$$\Omega^2(z) + \Omega(z) - \frac{z}{1-z} = 0 \quad \text{modulo } 2. \tag{2.1}$$

Proof. It is straightforward to see that

$$\Omega^2(z) = \sum_{e\ge0}\sum_{f\ge0} z^{2\cdot4^e(2f+1)} \quad \text{modulo } 2.$$

In plain words, this is the sum of all monomials z^m, where m runs through all positive integers with an odd number of zeroes to the far right of their binary representation. Consequently, we have

$$\Omega^2(z) + \Omega(z) = \sum_{m\ge1} z^m = \frac{z}{1-z} \quad \text{modulo } 2.$$

This is equivalent to the claim. □

Remark 2. Clearly, Proposition 1 implies that $\Omega(z)$ is algebraic modulo *any* power of 2. In particular, we have

$$\left(\Omega^2(z) + \Omega(z) - \frac{z}{1-z}\right)^N = 0 \quad \text{modulo } 2^N, \tag{2.2}$$

a relation that we shall use later on.

We now turn our attention to the derivative of the basic series $\Omega(z)$. By straightforward differentiation, we obtain

$$\Omega'(z) = \sum_{e\ge0} 4^e\left(\frac{z^{4^e-1}}{1-z^{2\cdot4^e}} + \frac{2z^{3\cdot4^e-1}}{(1-z^{2\cdot4^e})^2}\right). \tag{2.3}$$

We would like to prove that $\Omega'(z)$, when considered modulo a given power of 2, can be expressed as a polynomial in z and $(1-z)^{-1}$ with integer coefficients. The above relation does not quite achieve this, since the denominators on the right-hand side are not powers of $1-z$. However, the following is true.

On the other hand, by [5, Theorem VII.8], the coefficients of algebraic power series *do* have asymptotic formulae (whose form can even be described very specifically). Consequently, the series $\Omega(z)$ cannot be algebraic.

Lemma 3. *For all non-negative integers j and positive integers α and β, we have*

$$\frac{1}{(1+z^{2^j})^\alpha} = \operatorname{Pol}^+_{j,\alpha,\beta}\left(z,(1-z)^{-1}\right) \quad \text{modulo } 2^\beta,$$

where $\operatorname{Pol}^+_{j,\alpha,\beta}\left(z,(1-z)^{-1}\right)$ *is a polynomial in z and $(1-z)^{-1}$ with integer coefficients.*

Proof. We perform an induction with respect to $j+\beta$. For $j=0$ and arbitrary β, we have

$$\frac{1}{(1+z)^\alpha} = \frac{1}{(1-z+2z)^\alpha} = (1-z)^{-\alpha}\sum_{k\ge0}\binom{\alpha+k-1}{k}2^k\frac{z^k}{(1-z)^k}.$$

When this is considered modulo 2^β for some fixed β, the sum on the right-hand side becomes finite and is indeed a polynomial in z and $(1-z)^{-1}$.

For the induction step with $j\ge1$, we write

$$\begin{aligned}
\frac{1}{(1+z^{2^j})^\alpha} &= \frac{1}{(1+z^{2^{j-1}})^{2\alpha}} + \frac{1}{(1+z^{2^j})^\alpha} - \frac{1}{(1+z^{2^{j-1}})^{2\alpha}}\\
&= \frac{1}{(1+z^{2^{j-1}})^{2\alpha}} + \frac{1}{(1+z^{2^{j-1}})^{2\alpha}(1+z^{2^j})^\alpha}\left((1+z^{2^{j-1}})^{2\alpha}-(1+z^{2^j})^\alpha\right)\\
&= \frac{1}{(1+z^{2^{j-1}})^{2\alpha}} + \frac{1}{(1+z^{2^{j-1}})^{2\alpha}(1+z^{2^j})^\alpha}\\
&\qquad\times\left((1+2z^{2^{j-1}}+z^{2^j})^\alpha-(1+z^{2^j})^\alpha\right)\\
&= \frac{1}{(1+z^{2^{j-1}})^{2\alpha}} + \frac{1}{(1+z^{2^{j-1}})^{2\alpha}(1+z^{2^j})^\alpha}\\
&\qquad\times\sum_{\ell=1}^{\alpha}\binom{\alpha}{\ell}2^\ell\left(z^{2^{j-1}}\right)^\ell\left(1+z^{2^j}\right)^{\alpha-\ell}\\
&= \frac{1}{(1+z^{2^{j-1}})^{2\alpha}} + \sum_{\ell=1}^{\alpha}\binom{\alpha}{\ell}\frac{2^\ell z^{\ell\cdot2^{j-1}}}{(1+z^{2^{j-1}})^{2\alpha}(1+z^{2^j})^\ell}.
\end{aligned}$$

Now the induction hypothesis can be applied, and yields

$$\begin{aligned}
\frac{1}{(1+z^{2^j})^\alpha} &= \operatorname{Pol}^+_{j-1,2\alpha,\beta}\left(z,(1-z)^{-1}\right)\\
&\quad+\sum_{\ell=1}^{\alpha}\binom{\alpha}{\ell}2^\ell z^{\ell\cdot2^{j-1}}(\operatorname{Pol}^+)^{2\alpha}_{j-1,2\alpha,\beta-\ell}\left(z,(1-z)^{-1}\right)(\operatorname{Pol}^+)^{\ell}_{j,\ell,\beta-\ell}\left(z,(1-z)^{-1}\right)\\
&\hspace{10cm}\text{modulo } 2^\beta.
\end{aligned}$$

This completes the induction. ∎

Lemma 4. *For all non-negative integers j and positive integers α and β, we have*

$$\frac{1}{(1-z^{2^j})^\alpha} = \operatorname{Pol}_{j,\alpha,\beta}\left(z,(1-z)^{-1}\right) \quad \text{modulo } 2^\beta,$$

where $\operatorname{Pol}_{j,\alpha,\beta}\left(z,(1-z)^{-1}\right)$ *is a polynomial in z and $(1-z)^{-1}$ with integer coefficients.*

Proof. We perform an induction on j. Clearly, there is nothing to prove for $j=0$.

For the induction step, we write

$$\frac{1}{(1-z^{2^j})^\alpha} = \frac{1}{(1+z^{2^{j-1}})^\alpha} \cdot \frac{1}{(1-z^{2^{j-1}})^\alpha}.$$

By Lemma 3, we know that the first factor on the right-hand is a polynomial in z and $(1-z)^{-1}$, while the induction hypothesis guarantees that the second factor is such a polynomial as well. □

Identity (2.3) and Lemma 4 together imply our claim concerning $\Omega'(z)$ (it should be observed that, modulo a given 2-power 2^β, the sum on the right-hand side of (2.3) is finite).

Corollary 5. *The series $\Omega'(z)$, when coefficients are reduced modulo 2^β for some fixed β, can be expressed as a polynomial in z and $(1-z)^{-1}$ with integer coefficients.*

3. The method

We consider a (formal) differential equation of the form

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0, \tag{3.1}$$

where $\mathcal{P}$ is a polynomial with integer coefficients, which has a unique power series solution $F(z)$ with integer coefficients when the equation is considered modulo any fixed power of 2. (In the literature, series obeying a polynomial relation of the form (3.1) are known as *differentially algebraic* series; see, for instance, [2].) In this situation, we propose the following algorithmic approach to determining $F(z)$ modulo a 2-power 2^{2^α}, for some positive integer α. Let us fix a positive integer γ. We make the Ansatz

$$F(z) = \sum_{i=0}^{2^{\alpha+1}-1} a_i(z)\Omega^i(z^\gamma) \quad \text{modulo } 2^{2^\alpha}, \tag{3.2}$$

where $\Omega(z)$ is given by (1.2), and where the $a_i(z)$'s are (at this point) undetermined elements of $\mathbb{Z}[z, z^{-1}, (1-z^\gamma)^{-1}]$. Now we substitute (3.2) into (3.1), and we shall gradually determine approximations $a_{i,\beta}(z)$ to $a_i(z)$ such that (3.1) holds modulo 2^β, for $\beta = 1, 2, \dots, 2^\alpha$. To initiate the procedure, we consider the differential equation (3.1) modulo 2, with

$$F(z) = \sum_{i=0}^{2^{\alpha+1}-1} a_{i,1}(z)\Omega^i(z^\gamma) \quad \text{modulo } 2. \tag{3.3}$$

By Corollary 5, we know that $\Omega'(z^\gamma)$, when considered modulo 2, is in $\mathbb{Z}[z, (1-z^\gamma)^{-1}]$. Consequently, we see that the left-hand side of (3.1) is a polynomial in $\Omega(z^\gamma)$ with coefficients in $\mathbb{Z}[z, z^{-1}, (1-z^\gamma)^{-1}]$. We reduce powers $\Omega^k(z^\gamma)$ with $k \ge 2^{\alpha+1}$ using the relation

$$\left(\Omega^2(z^\gamma) + \Omega(z^\gamma) - \frac{z^\gamma}{1-z^\gamma}\right)^{2^\alpha} = 0 \quad \text{modulo } 2^{2^\alpha}, \tag{3.4}$$

which is the special case $N = 2^\alpha$ of (2.2). Since, at this point, we are only interested in finding a solution to (3.1) modulo 2, Relation (3.4) simplifies to

$$\Omega^{2^{\alpha+1}}(z^\gamma) + \Omega^{2^\alpha}(z^\gamma) - \frac{z^{\gamma\cdot 2^\alpha}}{(1-z^\gamma)^{2^\alpha}} = 0 \quad \text{modulo } 2. \tag{3.5}$$

Now we compare coefficients of powers $\Omega^k(z^\gamma)$, $k = 0, 1, \dots, 2^{\alpha+1} - 1$. This yields a system of $2^{\alpha+1}$ (differential) equations (modulo 2) for unknown functions $a_{i,1}(z)$ in $\mathbb{Z}[z, z^{-1}, (1 - z^\gamma)^{-1}]$, for $i = 0, 1, \dots, 2^{\alpha+1} - 1$, which may or may not have a solution.

Provided we have already found functions $a_{i,\beta}(z)$ in $\mathbb{Z}[z, z^{-1}, (1-z^\gamma)^{-1}]$, $i = 0, 1, \dots, 2^{\alpha+1} - 1$, for some β with $1 \le \beta \le 2^\alpha - 1$, such that

$$F(z) = \sum_{i=0}^{2^{\alpha+1}-1} a_{i,\beta}(z)\Omega^i(z^\gamma) \tag{3.6}$$

solves (3.1) modulo 2^β, we put

$$a_{i,\beta+1}(z) := a_{i,\beta}(z) + 2^\beta b_{i,\beta+1}(z), \quad i = 0, 1, \dots, 2^{\alpha+1} - 1, \tag{3.7}$$

where the $b_{i,\beta+1}(z)$'s are (at this point) undetermined elements in $\mathbb{Z}[z, z^{-1}, (1 - z^\gamma)^{-1}]$. Next we substitute

$$F(z) = \sum_{i=0}^{2^{\alpha+1}-1} a_{i,\beta+1}(z)\Omega^i(z^\gamma) \tag{3.8}$$

in (3.1) and consider the result modulo $2^{\beta+1}$. Using Corollary 5 and Lemma 4, we see that derivatives of $\Omega(z^\gamma)$, when considered modulo $2^{\beta+1}$, can be expressed as polynomials in z and $(1 - z^\gamma)^{-1}$. Consequently, we may expand the left-hand side of (3.1) as a polynomial in $\Omega(z^\gamma)$ with coefficients in $\mathbb{Z}[z, z^{-1}, (1 - z^\gamma)^{-1}]$. Subsequently, we apply again the reduction using Relation (3.4). By comparing coefficients of powers $\Omega^k(z^\gamma)$, $k = 0, 1, \dots, 2^{\alpha+1} - 1$, we obtain a system of $2^{\alpha+1}$ (differential) equations (modulo $2^{\beta+1}$) for the unknown functions $b_{i,\beta+1}(z)$, $i = 0, 1, \dots, 2^{\alpha+1} - 1$, which may or may not have a solution. If we manage to push this procedure through until $\beta = 2^\alpha - 1$, then, setting $a_i(z) = a_{i,2^\alpha}(z)$, $i = 0, 1, \dots, 2^{\alpha+1} - 1$, the series $F(z)$ as given in (3.2) is a solution to (3.1) modulo 2^{2^α}, as required.

We should point out that, in order for the method to be meaningful, it is essential to assume that the differential equation (3.1), when considered modulo an arbitrary 2-power 2^e, determines the solution $F(z)$ *uniquely* modulo 2^e (which we do). Otherwise, our method could produce several different "solutions," and it might be difficult to decide which of them actually corresponds to the series $F(z)$ we are interested in.

4. Motzkin numbers

Let M_n be the n-th *Motzkin number*, that is, the number of lattice paths from $(0, 0)$ to $(n, 0)$ consisting of steps taken from the set $\{(1, 0), (1, 1), (1, -1)\}$ never running below the x-axis. It is well-known (cf. [11, Ex. 6.37]) that the generating function $M(z) = \sum_{n\ge0} M_n\, z^n$ is given by (1.1) and hence satisfies the functional equation

$$z^2M^2(z) + (z - 1)M(z) + 1 = 0. \tag{4.1}$$

Theorem 6. *Let $\Omega(z)$ be given by* (1.2), *and let α be some positive integer. Then the generating function $M(z) = \sum_{n\ge0} M_n\, z^n$ for the Motzkin numbers, reduced modulo 2^{2^α}, can be expressed as a polynomial in $\Omega(z^4)$ of the form*

$$M(z) = \sum_{i=0}^{2\cdot2^\alpha-1} a_i(z)\Omega^i(z^4) \quad \text{modulo } 2^{2^\alpha},$$

where the coefficients $a_i(z)$, $i = 0, 1, \dots, 2^{\alpha+1} - 1$, *are Laurent polynomials in* z *and* $1 - z$.

Proof. We apply a slight variation of the method from Section 3. We start by making the Ansatz (compare with (3.3))

$$M(z) = \sum_{i=0}^{2^{\alpha+1}-1} a_i(z)\Omega^i(z^4) \quad \text{modulo } 2^{2^\alpha},$$

where $\Omega(z)$ is given by (1.2), and where the $a_i(z)$'s are (at this point) undetermined Laurent polynomials in z and $1 - z$.

For the "base step" (that is, for $\beta = 1$), we claim that

$$M_1(z) = \sum_{k=1}^{\alpha+1} \frac{z^{2^k-2}}{(1-z)^{2^k-1}} + \frac{1-z}{z^2}\Omega^{2^\alpha}(z^4)$$

solves (4.1) modulo 2. Indeed, substitution of $M_1(z)$ in place of $M(z)$ on the left-hand side of (4.1) yields the expression

$$z^2\left(\sum_{k=1}^{\alpha+1} \frac{z^{2\cdot(2^k-2)}}{(1-z)^{2\cdot(2^k-1)}} + \frac{(1-z)^2}{z^4}\Omega^{2^{\alpha+1}}(z^4)\right) \\ + (z-1)\left(\sum_{k=1}^{\alpha+1} \frac{z^{2^k-2}}{(1-z)^{2^k-1}} + \frac{1-z}{z^2}\Omega^{2^\alpha}(z^4)\right) + 1 \quad \text{modulo } 2.$$

Now one uses the relation (3.5) to "get rid of" $\Omega^{2^{\alpha+1}}(z^4)$. This leads to the expression

$$z^2\left(\sum_{k=1}^{\alpha+1} \frac{z^{2\cdot(2^k-2)}}{(1-z)^{2\cdot(2^k-1)}} + \frac{(1-z)^2}{z^4}\Omega^{2^\alpha}(z^4) + \frac{(1-z)^2}{z^4}\frac{z^{4\cdot 2^\alpha}}{(1-z^4)^{2^\alpha}}\right) \\ + (z-1)\left(\sum_{k=1}^{\alpha+1} \frac{z^{2^k-2}}{(1-z)^{2^k-1}} + \frac{1-z}{z^2}\Omega^{2^\alpha}(z^4)\right) + 1 \\ = \sum_{k=1}^{\alpha+1} \frac{z^{2^{k+1}-2}}{(1-z)^{2^{k+1}-2}} + \frac{(1-z)^2}{z^2}\Omega^{2^\alpha}(z^4) + \frac{z^{2^{\alpha+2}-2}}{(1-z)^{2^{\alpha+2}-2}} \\ + \sum_{k=1}^{\alpha+1} \frac{z^{2^k-2}}{(1-z)^{2^k-2}} + \frac{(1-z)^2}{z^2}\Omega^{2^\alpha}(z^4) + 1 \quad \text{modulo } 2,$$

which is indeed 0 modulo 2.

After we have completed the "base step," we now proceed with the iterative steps described in Section 3. We consider the Ansatz (3.6)–(3.8), where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution $M_\beta(z) = \sum_{i=0}^{2^{\alpha+1}-1} a_{i,\beta}(z)\Omega^i(z^4)$ to (4.1) modulo 2^β. This Ansatz, substituted in (4.1), produces the congruence

$$z^2M_\beta^2(z) + (z-1)M_\beta(z) + 2^\beta(z-1)\sum_{i=0}^{2^{\alpha+1}-1} b_{i,\beta+1}(z)\Omega^i(z^4) + 1 = 0 \quad \text{modulo } 2^{\beta+1}.$$

By our assumption on $M_\beta(z)$, we may divide by 2^β. Comparison of powers of $\Omega(z^4)$ then yields a system of congruences of the form

$$(1-z)b_{i,\beta+1}(z) + \mathrm{Pol}_i(z) = 0 \quad \text{modulo } 2, \qquad i = 0,1,\dots,2^{\alpha+1}-1,$$

where $\mathrm{Pol}_i(z)$, $i = 0,1,\dots,2^{\alpha+1}-1$, are in $\mathbb{Z}[z,z^{-1},(1-z)^{-1}]$. This system being trivially uniquely solvable, we have proved that, for an arbitrary positive integer α, our (variant of the) algorithm of Section 3 will produce a solution $M_{2^{\alpha+1}}(z)$ to (4.1) modulo 2^{2^α} which is a polynomial in $\Omega(z^4)$ with coefficients that are in $\mathbb{Z}[z,z^{-1},(1-z)^{-1}]$. □

5. The generating function for Motzkin numbers modulo 8

We have implemented the algorithm described in the proof of Theorem 6.[2] If we apply it with $\alpha = 2$, then we obtain

$$\begin{aligned}\sum_{n\ge0} M_n\, z^n &= \frac{8z^{15}+8z^{11}+8z^9+8z^8+8z^5}{(1-z)^{19}} + \frac{4z^{10}+12z^9+12z^7}{(1-z)^{13}} \\
&\quad + \frac{2z^{10}+4z^8+12z^7+2z^6+12z^5+2z^4}{(1-z)^{11}} + \frac{z^6}{(1-z)^7} + \frac{z^2}{(1-z)^3} + \frac{1}{1-z} \\
&\quad + \frac{4z^{10}}{(1-z)^{11}}\Omega(z) + \left(\frac{8z^{10}}{(1-z)^{13}} + \frac{4z^8}{(1-z)^9} + \frac{2z^6}{(1-z)^7}\right)\Omega^2(z) \\
&\quad + \left(\frac{8z^8}{(1-z)^9} + \frac{8z^6}{(1-z)^9} + \frac{8z^4}{(1-z)^9} + \frac{4z^2}{(1-z)^7}\right)\Omega^3(z) \\
&\quad + \left(\frac{8z^{10}}{(1-z)^{11}} + \frac{8(z^9+z^8+z^6+z^4+z+1)}{(1-z)^{11}} + \frac{4z^4+12z+12z^{-1}}{(1-z)^5}\right. \\
&\quad \left. + \frac{2z^2+12z+6+12z^{-1}+2z^{-2}}{(1-z)^3} + \frac{15}{z} + \frac{1}{z^2}\right)\Omega^4(z) \\
&\quad + \left(\frac{8z^2}{(1-z)^3} + \frac{4z^{-2}}{(1-z)^3}\right)\Omega^5(z) + \left(\frac{8(z^3+1+z^{-1})}{(1-z)^5} + \frac{4z^{-2}}{(1-z)} + \frac{2}{z^2} + \frac{14}{z}\right)\Omega^6(z) \\
&\quad + \left(\frac{4}{z^2} + \frac{12}{z} + \frac{8}{1-z}\right)\Omega^7(z) \qquad \text{modulo } 16. \end{aligned} \tag{5.1}$$

We are aiming at congruences for the Motzkin numbers modulo 8, thus we need to reduce the above expression modulo 8. In order to do this efficiently, we introduce the error series $E(z)$ defined by the relation

$$\Omega^2(z) + \Omega(z) - \frac{z}{1-z} - 2E(z) = 0. \tag{5.2}$$

A straightforward computation shows that, explicitly, the series $E(z)$ is given by

$$E(z) = \sum_{\substack{e_1,f_1,e_2,f_2\ge0\\(e_1,f_1)\prec(e_2,f_2)}} z^{4^{e_1}(2f_1+1)+4^{e_2}(2f_2+1)}. \tag{5.3}$$

Here, the symbol $\prec$ refers to the lexicographic order on pairs of integers, i.e., $(e_1,f_1) \prec (e_2,f_2)$ if, and only if, $e_1 < e_2$, or $e_1 = e_2$ and $f_1 < f_2$.

[2] The *Mathematica* input files are freely available; see the Note at the end of the Introduction.

We combine three reductions: (1) powers of $\Omega(z^4)$ are reduced by means of (2.2) with $N=3$; (2) powers of $\Omega(z^4)$ are further reduced using Relation (5.2) (at the cost of introducing the error series $E(z)$); (3) coefficients are reduced modulo 8. The final result is

$$\begin{aligned} M(z) = \Bigg(&\frac{4(z+1)}{z^2}E(z^4)+\frac{7}{z^2}+\frac{1}{z}\\ &+\frac{2z^7+2z^6+6z^5+6z^4+6z^3+6z^2+2z+2}{1-z^8}\Bigg)\Omega(z^4)\\ &+\frac{4E(z^8)(z+1)}{z^2}-2E(z^4)\left(\frac{7}{z^2}+\frac{5}{z}+\frac{2}{1-z}\right)\\ &+\frac{\begin{matrix}(z^{15}+5z^{14}+7z^{13}+3z^{12}+3z^{11}+3z^{10}+5z^9+5z^8\\ \qquad +z^7+5z^6+3z^5+7z^4+3z^3+3z^2+z+1)\end{matrix}}{1-z^{16}}\\ &\text{modulo } 8. \end{aligned} \tag{5.4}$$

Here, we also used that $E^2(z^4)=E(z^8)$ modulo 2. (This explains the occurrence of $E(z^8)$ in the above expression.)

In order to proceed, we need to know how to extract coefficients of z^n from the series

$$E(z^4)\Omega(z^4),\ \Omega(z^4),\ \frac{1}{1-z^8}\Omega(z^4),\ E(z^4),\ \text{and}\ \frac{1}{1-z}E(z^4).$$

The next section is devoted to solving these problems.

6. Coefficient extraction

We begin with coefficient extraction from the error series $E(z)$. In all what follows, coefficients n_i will be assumed to be either 0 or 1.

Lemma 7. *For all non-negative integers n, we have*

$$\langle z^n\rangle\, E(z) \equiv \begin{cases} \chi(e>0)(1+2n_1)+n_2+n_3+3n_4+n_5+3n_6+n_7+\cdots \pmod 4,\\ \qquad\qquad \textit{if}\ \ n=4^e(1+n_1 2+n_2 2^2+\cdots+n_k 2^k),\\ 2\chi(e>0)+n_1+2n_2 \pmod 4,\\ \qquad\qquad \textit{if}\ \ n=2\cdot 4^e(1+n_1 2+n_2 2^2+\cdots+n_k 2^k), \end{cases} \tag{6.1}$$

where $\chi(\mathcal{A})=1$ if the assertion $\mathcal{A}$ holds true, and $\chi(\mathcal{A})=0$ otherwise.

Proof. We have to count the number of quadruples $(e_1,f_1;e_2,f_2)$, where e_1,e_2,f_1,f_2 are non-negative integers with $e_1<e_2$, or $e_1=e_2$ and $f_1<f_2$, such that

$$4^{e_1}(2f_1+1)+4^{e_2}(2f_2+1)=n.$$

We may write

$$n=4^{e_1}(2f_1+1)+4^{e_2}(2f_2+1)=4^{e_1}\big(2f_1+1+4^{e_2-e_1}(2f_2+1)\big). \tag{6.2}$$

Let first $n=1+n_1 2+n_2 2^2+\cdots+n_k 2^k$. Then, quadruples $(e_1,f_1;e_2,f_2)$ satisfying (6.2) must satisfy $e_1=0<e_2$. For given e_2, the possible numbers f_2 such that (6.2) is

satisfied with a suitable f_1 are $0, 1, \dots, F$, where

$$F = \left\lfloor \frac{1}{2}\left(\frac{n-1}{4^{e_2}} - 1\right)\right\rfloor .$$

Thus, the number of above quadruples equals

$$\begin{aligned}
\sum_{e_2>0} \left\lfloor \frac{1}{2}\left(\frac{n-1}{4^{e_2}} + 1\right)\right\rfloor &= \sum_{e_2\ge 1} \left\lfloor \frac{1}{2}\left(\frac{n_1 2 + n_2 2^2 + \cdots + n_k 2^k}{4^{e_2}} + 1\right)\right\rfloor \\
&= \sum_{e_2\ge 1} \left\lfloor \frac{n_1}{2^{2e_2}} + \frac{n_2}{2^{2e_2-1}} + \cdots + \frac{n_{2e_2}+1}{2} + n_{2e_2+1} + 2n_{2e_2+2} + \cdots + 2^{k-2e_2-1} n_k \right\rfloor \\
&= \sum_{e_2\ge 1} (n_{2e_2} + n_{2e_2+1} + 2n_{2e_2+2}) \pmod 4 \\
&= n_2 + n_3 + 3n_4 + n_5 + 3n_6 + n_7 + 3n_8 + \cdots \pmod 4. \qquad (6.3)
\end{aligned}$$

This is in agreement with the first case in (6.1) with $e = 0$.

Next let $n = 4^e(1+n_1 2+n_2 2^2+\cdots+n_k 2^k)$ with $e \ge 1$. Then the above arguments apply again (with $e_1 = e < e_2$). Furthermore, there are now also quadruples $(e_1, f_1; e_2, f_2)$ with $e_1 = e_2 < e$ satisfying (6.2). Modulo 4, the only ones which are relevant in our count are those with $e_1 = e_2 = e - 1$ and

$$2f_1 + 2f_2 + 2 = 4 + n_1 8 + \cdots + n_k 2^{k+2}.$$

The number of pairs (f_1, f_2) of non-negative integers with $f_1 < f_2$ satisfying this equation equals

$$1 + n_1 2 + \cdots + n_k 2^k \equiv 1 + 2n_1 \pmod 4.$$

If this is added to the right-hand side of (6.3), the resulting expression is in agreement with the first case of (6.1) with $e > 0$.

The last remaining case is $n = 2 \cdot 4^e(1 + n_1 2 + n_2 2^2 + \cdots + n_k 2^k)$. Here, quadruples $(e_1, f_1; e_2, f_2)$ satisfying (6.2) must necessarily satisfy $e_1 = e_2 \le e$. It is then easy to see that, modulo 4, the only quadruples relevant for our count are those with $e_1 = e_2 = e-1$ (which only exist if $e > 0$), whose number is congruent to 2 modulo 4, and those with $e_1 = e_2 = e$, whose number equals

$$n_1 + n_2 2 + \cdots + n_k 2^{k-1} \equiv n_1 + 2n_2 \pmod 4.$$

Both cases together lead to the claimed result corresponding to the second case in (6.1). □

Next, we turn to coefficient extraction from the series $E(z^4)/(1-z)$.

Lemma 8. *For all non-negative integers n with binary representation $n = n_0 + n_1 2 + n_2 2^2 + \cdots$, we have*

$$\begin{aligned}
\langle z^n\rangle\, E(z^4)\frac{1}{1-z} \equiv \sum_{e_2>0} &(n'_{2e_2+2} + n'_{2e_2+3})(n_2 + n_3 + n_4 + n_5 + \cdots + n_{2e_2+1}) \\
&+ \sum_{i\ge 1} (n_{2i+1} + 1) n_{2i+2} \pmod 2, \qquad (6.4)
\end{aligned}$$

where $n - 4 = n'_0 + n'_1 2 + n'_2 4 + \cdots$.

Proof. We have to count the number of quintuples $(e_1, f_1; e_2, f_2; g)$, where e_1, e_2, f_1, f_2, g are non-negative integers with $e_1 < e_2$, or $e_1 = e_2$ and $f_1 < f_2$, such that

$$4^{e_1+1}(2f_1+1) + 4^{e_2+1}(2f_2+1) + g = n.$$

Given e_2, the range of possible f_2's is $0, 1, \dots, F_2$, where

$$F_2 = \left\lfloor \frac{1}{2}\left(\frac{n-4}{4^{e_2+1}} - 1\right)\right\rfloor.$$

Given e_2, f_2, and $e_1 < e_2$, the range of possible f_1's is $0, 1, \dots, F_1$, where

$$F_1 = \left\lfloor \frac{1}{2}\left(\frac{n - 4^{e_2+1}(2f_2+1)}{4^{e_1+1}} - 1\right)\right\rfloor.$$

Thus, the number of above quintuples with $e_1 < e_2$ equals

$$\begin{aligned}
&\sum_{e_2>0}\sum_{f_2=0}^{F_2}\sum_{e_1=0}^{e_2-1}\left\lfloor \frac{1}{2}\left(\frac{n - 4^{e_2+1}(2f_2+1)}{4^{e_1+1}} + 1\right)\right\rfloor\\
&\quad= \sum_{e_2>0}\sum_{f_2=0}^{F_2}\sum_{e_1=0}^{e_2-1}\left(\left\lfloor \frac{1}{2}\left(\frac{n}{4^{e_1+1}} + 1\right)\right\rfloor - 2\cdot 4^{e_2-e_1-1}(2f_2+1)\right)\\
&\quad\equiv \sum_{e_2>0}\sum_{f_2=0}^{F_2}\sum_{e_1=0}^{e_2-1}(n_{2e_1+2} + n_{2e_1+3}) \pmod 2\\
&\quad\equiv \sum_{e_2>0}\sum_{f_2=0}^{F_2}(n_2 + n_3 + n_4 + n_5 + \dots + n_{2e_2+1}) \pmod 2\\
&\quad\equiv \sum_{e_2>0}(F_2+1)\cdot(n_2 + n_3 + n_4 + n_5 + \dots + n_{2e_2+1}) \pmod 2\\
&\quad\equiv \sum_{e_2>0}(n'_{2e_2+2} + n'_{2e_2+3})(n_2 + n_3 + n_4 + n_5 + \dots + n_{2e_2+1}) \pmod 2. \qquad (6.5)
\end{aligned}$$

where $n - 4 = n'_0 + n'_1 2 + n'_2 4 + \cdots$.

On the other hand, if $e_1 = e_2$, then we want to count all triples (e_1, f_1, f_2) of non-negative integers with $f_1 < f_2$ such that

$$2\cdot 4^{e_1+1}(f_1 + f_2 + 1) \le n.$$

Since the number of pairs (x, y) of non-negative integers with $x < y$ such that $x + y = k$ equals $\lfloor (k+1)/2 \rfloor$, the number of above triples equals

$$\sum_{e_1\ge 0}\sum_{k=0}^{F}\left\lfloor \frac{k+1}{2}\right\rfloor \tag{6.6}$$

where

$$F = \left\lfloor \frac{n}{2\cdot 4^{e_1+1}}\right\rfloor - 1.$$

If $m = m_0 + m_1 2 + m_2 4 + \cdots$, then it is not difficult to see that $\sum_{k=0}^{m}\lfloor (k+1)/2 \rfloor$ is odd if and only if $m \equiv 1 \pmod 4$. In symbols,

$$\sum_{k=0}^{m}\left\lfloor \frac{k+1}{2}\right\rfloor = m_0(m_1+1) \pmod 2. \tag{6.7}$$

Thus, modulo 2, the sum in (6.6) becomes

$$\sum_{e_1\ge 0}\sum_{k=0}^{F}\left\lfloor \frac{k+1}{2}\right\rfloor \equiv (n_3+1)n_4+(n_5+1)n_6+\cdots \pmod 2. \tag{6.8}$$

The sum of (6.5) and (6.8) then yields (6.4). □

Our next series to be considered is $\Omega(z)/(1-z^2)$.

Lemma 9. *For all non-negative integers n with binary representation $n=n_0+n_1 2+n_2 2^2+\cdots$, we have*

$$\langle z^n\rangle \frac{1}{1-z^2}\Omega(z)\equiv\begin{cases}1+n_1+2n_2 \pmod 4, & \text{if } n \text{ is odd,}\\ n_2+n_3+3n_4+n_5+3n_6+n_7+\cdots \pmod 4, & \text{if } n \text{ is even.}\end{cases} \tag{6.9}$$

Proof. We have to count the number of triples $(e_1,f_1;g)$, where e_1,f_1,g are non-negative integers such that

$$4^{e_1}(2f_1+1)+2g=n.$$

Let first $n=1+n_1 2+n_2 2^2+\cdots+n_k 2^k$. Then necessarily $e_1=0$, so that we want to count all non-negative integers f_1 with $f_1\le (n-1)/2$. Modulo 4, the number $(n-1)/2$ is congruent to n_1+2n_2. The number of possible f_1's is by 1 larger, and this observation explains the first case in (6.9).

Now let $n=n_1 2+n_2 2^2+\cdots+n_k 2^k$. Given $e_1>0$, the integer f_1 may range from 0 to F, where

$$F=\left\lfloor \frac{1}{2}\left(\frac{n}{4^{e_1}}-1\right)\right\rfloor.$$

Thus, the number of possible triples $(e_1,f_1;g)$ is

$$\begin{aligned}&\sum_{e_2>0}\left\lfloor \frac{1}{2}\left(\frac{n}{4^{e_1}}+1\right)\right\rfloor\\ &\quad=\sum_{e_2>0}\left\lfloor \frac{n_1}{2^{2e_1}}+\frac{n_2}{2^{2e_1-1}}+\cdots+\frac{n_{2e_1}+1}{2}+n_{2e_1+1}+2n_{2e_1+2}+\cdots+2^{k-2e_1-1}n_k\right\rfloor\\ &\quad\equiv\sum_{e_2>0}(n_{2e_1}+n_{2e_1+1}+2e_{2e_1+2}) \pmod 4\\ &\quad\equiv n_2+n_3+3n_4+n_5+3n_6+n_7+\cdots \pmod 4,\end{aligned}$$

as desired. □

Finally, we address coefficient extraction from the product $E(z)\Omega(z)$.

Lemma 10. *Let n be a non-negative integer.*

(1) *If $n=4^e(1+n_1 2+n_2 2^2+\cdots+n_k 2^k)$, then*

$$\begin{aligned}\langle z^n\rangle E(z)\,\Omega(z)&\equiv (n_1+1)n_2+\sum_{i\ge 1}n_{2i+1}(n_{2i+2}+1)+\chi(e\ge 1)\cdot(n_2+n_3+\cdots)\\ &\quad+\sum_{e_3>0}(n'_{2e_3}+n'_{2e_3+1})(n_2+n_3+n_4+n_5+\cdots+n_{2e_3-1}) \pmod 2, \end{aligned}\tag{6.10}$$

where $n4^{-e}-4=1+n'_1 2+n'_2 4+\cdots$.

(2) *If* $n = 2 \cdot 4^e(1 + n_1 2 + n_2 2^2 + \cdots + n_k 2^k)$, *then*

$$\langle z^n\rangle\, E(z)\, \Omega(z) \equiv \chi(e \ge 1) + (n_1+n_2) + (n_1+n_2+n_3+n_4+\cdots)(1+n_1) \pmod 2. \tag{6.11}$$

Proof. We have to count the number of sextuples $(e_1, f_1; e_2, f_2; e_3, f_3)$, where $e_1, e_2, f_1, f_2, e_3, f_3$ are non-negative integers with $(e_1, f_1) \prec (e_2, f_2)$, such that

$$4^{e_1}(2f_1 + 1) + 4^{e_2}(2f_2 + 1) + 4^{e_3}(2f_3 + 1) = n. \tag{6.12}$$

We need this number only modulo 2. By pairing up sextuples $(e_1, f_1; e_2, f_2; e_3, f_3)$ with $(e_1, f_1) \prec (e_3, f_3) \prec (e_2, f_2)$ with those sextuples with $(e_3, f_3) \prec (e_1, f_1) \prec (e_2, f_2)$, one sees that we may equivalently count all sextuples $(e_1, f_1; e_2, f_2; e_3, f_3)$ with $(e_1, f_1) \preceq (e_2, f_2) \preceq (e_3, f_3)$, but not all three equal, satisfying (6.12). In the remainder of this proof, we shall always assume these conditions.

Case 1: $n = 4^e(1 + n_1 2 + n_2 2^2 + \cdots + n_k 2^k)$. Here, we have to consider all possible cases for solutions to (6.12) to exist: (a) $e_1 = e_2 = e_3 = e$; (b) $0 \le e_1 = e < e_2 = e_3$; (c) $0 \le e_1 = e < e_2 < e_3$; (d) $0 \le e_1 = e_2 < e_3$.

(a) Writing $n = 4^e u$, we see that (6.12) reduces to

$$f_1 + f_2 + f_3 = \frac{u-3}{2}, \tag{6.13}$$

with $f_1 \le f_2 \le f_3$ but not all three equal. Let us denote the number of triples (f_1, f_2, f_3) with $f_1 + f_2 + f_3 = N$, $f_1 \le f_2 \le f_3$, not all three equal, by $f(N)$. In order to compute $f(N)$, we face a classical partition problem, namely the problem of counting all integer partitions of N with at most three parts, not all of them equal. It is then folklore (cf. [1, Sec. 3.2]) that, for the generating function we have

$$\sum_{N=0}^{\infty} f(N)\, z^N = \frac{1}{(1-z)(1-z^2)(1-z^3)} - \frac{1}{1-z^3} = \frac{z + z^2 - z^3}{(1-z)(1-z^2)(1-z^3)}.$$

Modulo 2, this reduces to

$$\sum_{N=0}^{\infty} f(N)\, z^N = \frac{z}{1-z^4} \qquad \text{modulo } 2.$$

In other words, $f(N) \equiv 1 \pmod 2$ if, and only if, $N \equiv 1 \pmod 4$. Returning to our problem of counting triples satisfying (6.13) modulo 2, this means that the number of the above triples is odd if, and only if, $u \equiv 5 \pmod 8$. Hence, a slick way to express this number of triples modulo 2 in terms of the binary digits of u is

$$n_0(n_1 + 1)n_2 = (n_1 + 1)n_2 \pmod 2. \tag{6.14}$$

(b) With the convention $n = 4^e u$ from above, we see that we have to count all triples (e_2, f_2, f_3) with $e_2 > e$ and $f_2 \le f_3$ satisfying

$$2 \cdot 4^{e_2 - e}(f_2 + f_3 + 1) \le u - 1.$$

Since the number of pairs (x, y) of non-negative integers with $x \le y$ such that $x + y = k$ equals $\lfloor (k+2)/2 \rfloor$, the number of above triples equals

$$\sum_{e_2 > e} \sum_{k=0}^{F} \left\lfloor \frac{k+2}{2} \right\rfloor \tag{6.15}$$

where

$$F = \left\lfloor \frac{u-1}{2 \cdot 4^{e_2-e}} \right\rfloor - 1.$$

Using (6.7) again, the sum in (6.15), when reduced modulo 2, becomes

$$\sum_{e_2>e} \sum_{k=0}^{F} \left\lfloor \frac{k+2}{2} \right\rfloor \equiv n_3(n_4+1) + n_5(n_6+1) + \cdots \pmod 2. \tag{6.16}$$

(c) With the same notation as above, here we have to count all quadruples $(e_2, f_2; e_3, f_3)$ with $e < e_2 < e_3$ satisfying

$$4^{e_2-e}(2f_2+1) + 4^{e_3-e}(2f_3+1) \le u-1.$$

Given e_3 with $e_3 > e$, the range of possible f_3's is $0, 1, \dots, F_3$, where

$$F_3 = \left\lfloor \frac{1}{2} \left(\frac{u-5}{4^{e_3-e}} - 1 \right) \right\rfloor.$$

Given e_3, f_3, and e_2 with $e < e_2 < e_3$, the range of possible f_2's is $0, 1, \dots, F_2$, where

$$F_2 = \left\lfloor \frac{1}{2} \left(\frac{u - 4^{e_3-e}(2f_3+1) - 1}{4^{e_2-e}} - 1 \right) \right\rfloor.$$

Thus, the number of above quadruples with $e_2 < e_3$ equals

$$\begin{aligned}
&\sum_{e_3>e} \sum_{f_3=0}^{F_3} \sum_{e_2=e+1}^{e_3-1} \left\lfloor \frac{1}{2} \left(\frac{u - 4^{e_3-e}(2f_3+1) - 1}{4^{e_2-e}} + 1 \right) \right\rfloor \\
&\quad = \sum_{e_3>e} \sum_{f_3=0}^{F_3} \sum_{e_2=e+1}^{e_3-1} \left(\left\lfloor \frac{1}{2} \left(\frac{u-1}{4^{e_2-e}} + 1 \right) \right\rfloor - 2 \cdot 4^{e_3-e_2-1}(2f_3+1) \right) \\
&\quad \equiv \sum_{e_3>e} \sum_{f_3=0}^{F_3} \sum_{e_2=e+1}^{e_3-1} (n_{2e_2-2e} + n_{2e_2-2e+1}) \pmod 2 \\
&\quad \equiv \sum_{e_3>e} \sum_{f_3=0}^{F_3} (n_2 + n_3 + n_4 + n_5 + \cdots + n_{2e_3-2e-1}) \pmod 2 \\
&\quad \equiv \sum_{e_3>e} (F_3+1) \cdot (n_2 + n_3 + n_4 + n_5 + \cdots + n_{2e_3-2e-1}) \pmod 2 \\
&\quad \equiv \sum_{e_3>e} (n'_{2e_3-2e} + n'_{2e_3-2e+1})(n_2 + n_3 + n_4 + n_5 + \cdots + n_{2e_3-2e-1}) \pmod 2,
\end{aligned} \tag{6.17}$$

where $u - 4 = 1 + n'_1 2 + n'_2 4 + \cdots$.

(d) Here, Equation (6.12) reduces to

$$(f_1 + f_2 + 1) + 2 \cdot 4^{e_3-e_1-1}(2f_3+1) = 2 \cdot 4^{e-e_1-1} u. \tag{6.18}$$

From this equation it is obvious that $e_1 \le e-1$. Since the second term on the left-hand side is divisible by 2 because of $e_3 > e_1$, the sum $f_1 + f_2 + 1$ must also be divisible by 2. We need not consider the case where $f_1 + f_2 + 1 \equiv 0 \pmod 4$ since then the number of possible pairs (f_1, f_2) with $f_1 \le f_2$ is even. Thus, we may assume that

$f_1+f_2+1 \equiv 2 \pmod 4$, in which case the number of possible pairs (f_1, f_2) with $f_1 \le f_2$ is odd. Inspecting (6.18) under this assumption again, we conclude that $e_3 \ge e+1$.

The counting problem that remains to be solved (modulo 2) hence is to count all pairs (e_3, f_3) with $e_3 \ge e+1$ satisfying

$$4^{e_3}(2f_3+1) \le 4^e \cdot u. \tag{6.19}$$

Given e_3, the integer f_3 ranges between 0 and F_3, where

$$F_3 = \left\lfloor \frac{1}{2}\left(\frac{u}{4^{e_3-e}} - 1\right)\right\rfloor .$$

The number of pairs (e_3, f_3) satisfying (6.19) then is

$$\begin{aligned}\sum_{e_3>e}(F_3+1) &= \sum_{e_3>e}\left\lfloor \frac{1}{2}\left(\frac{u}{4^{e_3-e}} + 1\right)\right\rfloor \\ &\equiv \sum_{e_3>e}(n_{2e_3-2e} + n_{2e_3-2e+1}) \pmod 2 \\ &\equiv n_2 + n_3 + \cdots \pmod 2. \end{aligned}\tag{6.20}$$

It should be noted that, since in the current case $0 \le e_1 \le e-1$, we must have $e \ge 1$ in order that (6.20) can actually occur. The contribution of Subcase (d) to the final result therefore is

$$\chi(e \ge 1)\cdot(n_2+n_3+\cdots) \pmod 2. \tag{6.21}$$

Adding up the individual contributions (6.14), (6.16), (6.17), and (6.21), we arrive at the right-hand side of (6.10).

Case 2: $n = 2\cdot 4^e(1+n_1 2+n_2 2^2+\cdots+n_k 2^k)$. In order to have solutions to (6.12) (with $(e_1, f_1) \preceq (e_2, f_2) \preceq (e_3, f_3)$, but not all three equal, as we assume throughout), we must have $0 \le e_1 = e_2 < e_3$. In that case, Equation (6.12) reduces to

$$2\cdot 4^{e_1}(f_1+f_2+1) + 4^{e_3}(2f_3+1) = n = 2\cdot 4^e \cdot u, \tag{6.22}$$

where u is some odd number.

Let us for the moment fix the sum of f_1+f_2+1 to equal k, say. If this number is divisible by 4, say $k=4k'$, then the number of possible pairs f_1, f_2 with $f_1 \le f_2$ and $f_1+f_2+1 = 4k'$ is $\lfloor (4k'+1)/2\rfloor = 2k'$, which is even. Since we are only interested in numbers of solutions modulo 2, we may disregard these cases.

There are two possibilities which remain to be considered: either

$$f_1+f_2+1 = 2u_0+1 \tag{6.23}$$

for some $u_0 \ge 0$, or

$$f_1+f_2+1 = 2(2u_0+1) \tag{6.24}$$

for some $u_0 \ge 0$.

In the first case, that is, if (6.23) holds, then, from (6.12), we obtain

$$2\cdot 4^{e_1}(2u_0+1) + 4^{e_3}(2f_3+1) = n = 2\cdot 4^e\cdot u,$$

for some odd positive integer u. Because of $e_1 < e_3$, this implies $e_1 = e$.

Given e_3 with $e_3 > e$, the range of possible f_3's is $0, 1, \dots, F_3$, where

$$F_3 = \left\lfloor \frac{1}{2}\left(\frac{n}{4^{e_3}} - 1\right)\right\rfloor .$$

Given $e_3 > e$ and f_3, the numbers e_1 and u_0 are uniquely determined (recall that $e_1 = e$). Since the number of pairs (f_1, f_2) with $f_1 \le f_2$ satisfying (6.23) equals $\left\lfloor \frac{1}{2}\big((2u_0+1)+1\big)\right\rfloor = u_0+1$, the number of solutions to (6.12) which we have to consider in the current case is

$$
\begin{aligned}
\sum_{e_3>e}\sum_{f_3=0}^{F_3}(u_0+1) &= \sum_{e_3>e}\sum_{f_3=0}^{F_3}\left\lfloor \frac{1}{2}\left(\frac{n-4^{e_3}(2f_3+1)}{2\cdot 4^e}+1\right)\right\rfloor \\
&= \sum_{e_3>e}\sum_{f_3=0}^{F_3}\left(\left\lfloor \frac{1}{2}\left(\frac{n}{2\cdot 4^e}+1\right)\right\rfloor - 4^{e_3-e-1}(2f_3+1)\right) \\
&\equiv \sum_{e_3>e}(F_3+1)\left(\left\lfloor \frac{1}{2}\left(\frac{n}{2\cdot 4^e}+1\right)\right\rfloor - \chi(e_3=e+1)\right) \pmod 2 \\
&\equiv \sum_{e_3>e}(n_{2e_3-2e-1}+n_{2e_3-2e})\left((1+n_1)-\chi(e_3=e+1)\right) \pmod 2 \\
&\equiv (n_1+n_2+n_3+\cdots)(1+n_1)-(n_1+n_2) \pmod 2. \qquad (6.25)
\end{aligned}
$$

In the second case, that is, if (6.24) holds, then the number of possible pairs (f_1, f_2) with $f_1 \le f_2$ satisfying (6.24) equals $\left\lfloor \frac{1}{2}\big(2(2u_0+1)+1\big)\right\rfloor = 2u_0+1$, which is odd. Since we are only interested in the number of solutions to (6.12) modulo 2, we may therefore simply continue with u_0, and determine the number of quadruples (e_1, u_0, e_3, f_3) for which

$$4^{e_1+1}(2u_0+1) + 4^{e_3}(2f_3+1) = 2\cdot 4^e\cdot u,$$

for some odd positive integer u. Because of $e_1 < e_3$, it follows that $e_1+1 = e_3$. Thus, the above relation becomes

$$u_0 + f_3 + 1 = 4^{e_3-e}\cdot u.$$

There is no relation between u_0 and f_3, hence the number of pairs (u_0, f_3) satisfying the above relation equals the right-hand side, which is $4^{e_3-e}u$. This quantity is odd if, and only if, we have $e_3 = e$. Since $e_3 = e_1 + 1 \ge 1$, the contribution of the current case is $\chi(e \ge 1)$. If we add this to the earlier contribution (6.25), then we obtain the right-hand side of (6.11).

This completes the proof of the lemma. □

7. Motzkin numbers modulo 8

Using the auxiliary results from Section 6 in (5.4), we are now able to provide explicit formulae for the congruence class of M_n modulo 8 in terms of the binary digits of n.

Theorem 11. *Let n be a positive integer with binary expansion*

$$n = n_0 + n_1\cdot 2 + n_2\cdot 2^2 + \cdots .$$

Furthermore, let K denote the least integer ≥ 4 such that $n_K = 0$. The Motzkin numbers M_n satisfy the following congruences modulo 8:

$$M_n \equiv_8 \begin{cases} 2s_2^2(n) + 4e_2(n) + 1, & \text{if } n \equiv 0 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 3, & \text{if } n \equiv 1 \pmod{16},\\ 4s_2(n) + 6, & \text{if } n \equiv 2 \pmod{16},\\ 4, & \text{if } n \equiv 3 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 3, & \text{if } n \equiv 4 \pmod{16},\\ 2s_2^2(n) + 4e_2(n) + 5, & \text{if } n \equiv 5 \pmod{16},\\ 6s_2^2(n) + 4n_4\, s_2(n) + 4e_2(n) + 2n_4 + 7, & \text{if } n \equiv 6 \pmod{16},\\ 2s_2^2(n) + 4n_4\, s_2(n) + 4e_2(n) + 2n_4 + 5, & \text{if } n \equiv 7 \pmod{16},\\ 2s_2^2(n) + 4e_2(n) + 1, & \text{if } n \equiv 8 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 3, & \text{if } n \equiv 9 \pmod{16},\\ 4, & \text{if } n \equiv 10 \pmod{16},\\ 4s_2(n) + 2, & \text{if } n \equiv 11 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 3, & \text{if } n \equiv 12 \pmod{16},\\ 2s_2^2(n) + 4e_2(n) + 5, & \text{if } n \equiv 13 \pmod{16},\\ (n_{K+1} + 1)(4s_2(n) + 6), & \text{if } n \equiv 14 \pmod{16} \text{ and } K \text{ is even},\\ 2n_{K+1} + 4n_{K+1}s_2(n) + 2s_2^2(n) + 4s_2(n) + 4e_2(n) + 7, & \\ & \text{if } n \equiv 14 \pmod{16} \text{ and } K \text{ is odd},\\ 6n_{K+1} + 4n_{K+1}s_2(n) + 4, & \text{if } n \equiv 15 \pmod{16} \text{ and } K \text{ is even},\\ 2n_{K+1} + 4n_{K+1}s_2(n) + 2s_2^2(n) + 4e_2(n) + 5, & \\ & \text{if } n \equiv 15 \pmod{16} \text{ and } K \text{ is odd}. \end{cases}$$

Here, $s_2(n)$ denotes the sum of the binary digits of n, while $e_2(n)$ denotes the number of pairs of successive digits in the binary expansion of n, with both digits equalling 1. *The symbol $x \equiv_8 y$ is short for $x \equiv y$* (mod 8)*.*

Sketch of proof. We have to discuss 16 different cases depending on the congruence class of n modulo 16. Since the arguments in all these cases are very similar, we content ourselves with presenting the most complex case in detail, leaving the remaining cases to the reader.

Let $n \equiv 15 \pmod{16}$, and let L be the least integer $\ge K + 2$ with $n_L \ne 0$. In other words, the binary representation of the number n is of the form

$$(n)_2 = \dots \overset{\overset{L}{\downarrow}}{1}0 \dots 0 n_{K+1} \overset{\overset{K}{\downarrow}}{0}1 \dots 1 \vdots 1111. \tag{7.1}$$

(The vertical dots separate significant digits from the four 1's on the right making n a number congruent to 15 modulo 16. Otherwise, these dots may be safely ignored.)

Let first K be even, say $K = 2k$. For our specific n, we extract the coefficient of z^n in (5.4). The relevant terms are

$$4z^{-1}E(z^4)\Omega(z^4),\ z^{-1}\Omega(z^4),\ \frac{6z^3}{1-z^8}\Omega(z^4),\ \frac{2z^7}{1-z^8}\Omega(z^4),\\ 4z^{-1}E(z^8),\ -10z^{-1}E(z^4),\ -\frac{4}{1-z}E(z^4),\ \frac{z^{15}}{1-z^{16}}. \tag{7.2}$$

Coefficient extraction for these terms is discussed in Lemmas 10, 9, 7, and 8, respectively (ordered according to the order of the terms in (7.2)). Adding all contributions, we obtain

$$\begin{aligned}4(n_{2k+1}+1)n_{2k+2} &+ 4\sum_{i\ge k+1} n_{2i+1}(n_{2i+2}+1) + 4\sum_{i\ge 2k+2} n_i\\ &+ 4\sum_{e>k}(n'_{2e}+n'_{2e+1})(n_{2k+2}+n_{2k+3}+\cdots+n_{2e-1})\\ +1+6(2+2n_4) &+ 2(n_4+n_5+3n_6+n_7+3n_8+n_9+\cdots)+4(2+n_{2k+1}+2n_{2k+2})\\ &+ 6(1+2n_{2k+1}+n_{2k+2}+n_{2k+3}+3n_{2k+4}+n_{2k+5}+3n_{2k+6}+n_{2k+7}+\cdots)\\ &+ 4\sum_{e>k}(n_{2e+2}+n_{2e+3})(n_2+n_3+\cdots+n_{2e+1})+4\sum_{i\ge1}(n_{2i+1}+1)n_{2i+2}+1,\end{aligned} \tag{7.3}$$

where the digits n'_j are defined by

$$(n+1)2^{-2k}-4 = 1 + n'_{2k+1}2 + n'_{2k+2}4 + \cdots .$$

In order to control the auxiliary digits n'_j, we have to distinguish between L (recall (7.1)) being even or odd. If this is done, one sees that one may simply drop the primes without changing the result.

Next, we observe that

$$n_2+n_3+\cdots+n_{2k+1} \equiv 1+n_{2k+1} \pmod 2.$$

Using this, we may split the first sum in the last line of (7.3) in the following way:

$$\begin{aligned}4\sum_{e>k}&(n_{2e+2}+n_{2e+3})(n_2+n_3+\cdots+n_{2e+1})\\ &\equiv 4\sum_{e>k}(n_{2e+2}+n_{2e+3})(1+n_{2k+1})\\ &\qquad + 4\sum_{e>k}(n_{2e+2}+n_{2e+3})(n_{2k+2}+n_{2k+3}+\cdots+n_{2e+1}) \pmod 8\\ &\equiv 4(1+n_{2k+1})\sum_{i\ge 2k+4} n_i + 4\sum_{e>k}(n_{2e+2}+n_{2e+3})(n_{2k+2}+n_{2k+3}+\cdots+n_{2e+1})\\ &\qquad \pmod 8.\end{aligned} \tag{7.4}$$

The last sum in this expression cancels with the sum in the second line of (7.3), when reduced modulo 8, except for the term for $e = k+1$.

A similar partial cancellation, modulo 8, takes place between the big terms in parentheses in the third and fourth lines of (7.3).

For the first sum in the first line and the last sum in the last line, we observe that

$$\begin{aligned} 4\sum_{i\ge k+1} n_{2i+1}(n_{2i+2}+1)+4\sum_{i\ge1}(n_{2i+1}+1)n_{2i+2}\\ &= 4\sum_{i\ge k+1} n_{2i+1}n_{2i+2}+4\sum_{i\ge k+1} n_{2i+1}+4\sum_{i\ge1} n_{2i+1}n_{2i+2}+4\sum_{i\ge1} n_{2i+2}\\ &\equiv 4\sum_{i=1}^{k} n_{2i+1}n_{2i+2}+4\sum_{i\ge 2k+2} n_i+4\sum_{i=1}^{k} n_{2i+2}\pmod 8\\ &\equiv 4(k-2+n_{2k+1}n_{2k+2})+4\sum_{i\ge 2k+2} n_i+4(k-2+n_{2k+2})\pmod 8\\ &\equiv 4(n_{2k+1}+1)n_{2k+2}+4\sum_{i\ge 2k+2} n_i\pmod 8. \end{aligned}$$

After further simplification, one obtains the claimed expression $6n_{K+1}+4n_{K+1}s_2(n)+4$.

Now let K be odd, say $K=2k+1$. The relevant terms from which one extracts the coefficient of z^n are again the ones in (7.2). However, the relevant cases in Lemmas 10 and 7 are not the same. More precisely, here we obtain

$$\begin{aligned} 4+4n_{2k+2}+4n_{2k+3}+4(n_{2k+2}+1)\sum_{i\ge 2k+2} n_i\\ +0+6(2+2n_4)+2(n_4+n_5+3n_6+n_7+3n_8+n_9+\cdots)\\ +4(1+2n_{2k+2}+n_{2k+3}+n_{2k+4}+3n_{2k+5}+n_{2k+6}+3n_{2k+7}+n_{2k+8}+\cdots)\\ +6(2+n_{2k+2}+2n_{2k+3})+4\sum_{e>k}(n_{2e+2}+n_{2e+3})(n_2+n_3+\cdots+n_{2e+1})\\ +4\sum_{i\ge1}(n_{2i+1}+1)n_{2i+2}+1. \end{aligned}\tag{7.5}$$

This expression can be simplified in much the same way as (7.3); with one notable difference though. The sums in the next-to-last and the last lines have no counterparts (as opposed to the situation in (7.3)). Consequently, they need a different treatment.

The sum in the next-to-last line of (7.5) is first transformed in the same way as before, see (7.4). Then one observes that

$$
\begin{aligned}
&4\sum_{e>k}(n_{2e+2}+n_{2e+3})(n_{2k+2}+n_{2k+3}+\cdots+n_{2e+1})\\
&\quad=4\sum_{i>j\ge 2k+2}n_in_j-4\sum_{i\ge k+1}n_{2i}n_{2i+1}\\
&\quad=2\Bigg(\sum_{i\ge 2k+2}n_i\Bigg)^2-2\sum_{i\ge 2k+2}n_i-4\sum_{i\ge k+1}n_{2i}n_{2i+1}\\
&\quad=2\Bigg(s_2(n)-\sum_{i=0}^{2k+1}n_i\Bigg)^2-2\sum_{i\ge 2k+2}n_i-4\sum_{i\ge k+1}n_{2i}n_{2i+1}\\
&\quad\equiv 2s_2^2(n)-4n_{2k+1}s_2(n)+2n_{2k+1}-2\sum_{i\ge 2k+2}n_i-4\sum_{i\ge k+1}n_{2i}n_{2i+1}\pmod 8.
\end{aligned}
$$

The last sum combines with the sum $4\sum_{i\ge1}n_{2i+1}n_{2i+2}$ appearing in the last line of (7.5) into $4e_2(n)$, up to some error that can be computed explicitly modulo 8. We leave the remaining simplifications, leading to the claimed expression

$$2n_{2k+2}+4n_{2k+2}s_2(n)+2s_2^2(n)+4e_2(n)+5,$$

to the reader. □

The following result of Eu, Liu and Yeh [4], characterising even congruence classes of M_n modulo 8, can now readily be obtained through a straightforward case-by-case analysis using the corresponding cases from Theorem 11.

Corollary 12. *The Motzkin number M_n is even if, and only if, $n=(4i+\varepsilon)4^{j+1}-\delta$ for non-negative integers i,j, $\varepsilon=1,3$, and $\delta=1,2$. Moreover, we have*

$$M_n\equiv_8\begin{cases}4, & \text{if } (\varepsilon,\delta)=(1,1) \text{ or } (3,2),\\ 4y+2, & \text{if } (\varepsilon,\delta)=(1,2) \text{ or } (3,1),\end{cases}$$

where y is the number of 1's in the binary expansion of $4i+\varepsilon-1$.

Moreover, Theorem 11 allows us to provide a characterisation of all those n for which M_n lies in *any* specified congruence class modulo 8. As an example, we give the characterisation for the congruence class 1.

Corollary 13. *The Motzkin number M_n is congruent to 1 modulo 8 if, and only if, n satisfies one of the following conditions:*

(1) $n\equiv 0\pmod{16}$ *and* $s_2(n)\equiv e_2(n)\equiv 0\pmod 2$;
(2) $n\equiv 1\pmod{16}$, $s_2(n)\equiv 1\pmod 2$, *and* $e_2(n)\equiv 0\pmod 2$;
(3) $n\equiv 4\pmod{16}$, $s_2(n)\equiv 1\pmod 2$, *and* $e_2(n)\equiv 0\pmod 2$;
(4) $n\equiv 5\pmod{16}$, $s_2(n)\equiv 0\pmod 2$, *and* $e_2(n)\equiv 1\pmod 2$;
(5) $n\equiv 6\pmod{16}$, $n_4=0$, $s_2(n)\equiv e_2(n)\equiv 1\pmod 2$;
(6) $n\equiv 6\pmod{16}$, $n_4=1$, $s_2(n)\equiv e_2(n)\equiv 0\pmod 2$;
(7) $n\equiv 7\pmod{16}$, $n_4=0$, $s_2(n)\equiv 0\pmod 2$, *and* $e_2(n)\equiv 1\pmod 2$;
(8) $n\equiv 7\pmod{16}$, $n_4=1$, $s_2(n)\equiv e_2(n)\equiv 1\pmod 2$;
(9) $n\equiv 8\pmod{16}$, $s_2(n)\equiv e_2(n)\equiv 0\pmod 2$;

(10) $n \equiv 9 \pmod{16}$, $s_2(n) \equiv 1 \pmod 2$, *and* $e_2(n) \equiv 0 \pmod 2$;
(11) $n \equiv 12 \pmod{16}$, $s_2(n) \equiv 1 \pmod 2$, *and* $e_2(n) \equiv 0 \pmod 2$;
(12) $n \equiv 13 \pmod{16}$, $s_2(n) \equiv 0 \pmod 2$, *and* $e_2(n) \equiv 1 \pmod 2$;
(13) $n \equiv 14 \pmod{16}$, K *odd,* $n_{K+1} = 0$, $s_2(n) \equiv e_2(n) \equiv 1 \pmod 2$;
(14) $n \equiv 14 \pmod{16}$, K *odd,* $n_{K+1} = 1$, $s_2(n) \equiv e_2(n) \equiv 0 \pmod 2$;
(15) $n \equiv 15 \pmod{16}$, K *odd,* $n_{K+1} = 0$, $s_2(n) \equiv 0 \pmod 2$, *and* $e_2(n) \equiv 1 \pmod 2$;
(16) $n \equiv 15 \pmod{16}$, K *odd,* $n_{K+1} = 1$, $s_2(n) \equiv e_2(n) \equiv 1 \pmod 2$;

where $s_2(n)$, $e_2(n)$, *and* K *are defined as in Theorem* 11.

It should be observed that it is straightforward to generate all possible n in any of the 16 cases in the characterisation of the previous corollary. Characterisations similar to the one in Corollary 13 are available for all other congruence classes modulo 8.

We leave it as an open problem whether a description for the odd congruence classes of M_n modulo 8 exists which is comparably compact as the one of Eu, Liu and Yeh for the even ones, given here in Corollary 12. We do not hide that we are very sceptical about this.

8. Further applications

In this final section, we show that the same approach that we applied in Sections 4–7 to Motzkin numbers also works for the sequences of Motzkin prefix numbers, of Riordan numbers, of hex tree numbers, and of central trinomial coefficients. Since the arguments are completely analogous, we content ourselves with brief sketches of the main points and subsequent statements of the corresponding results for congruences modulo 8.

8.1. **Motzkin prefix numbers modulo 8.**

Let MP_n be the n-th *Motzkin prefix number*, that is, the number of lattice paths from $(0,0)$ consisting of n steps taken from the set $\{(1,0),(1,1),(1,-1)\}$ never running below the x-axis. Gouyou-Beauchamps and Viennot [6] have shown that MP_n also counts directed rooted animals with $n+1$ vertices. It is well-known (cf. e.g. [8, Sec. 8]) that the generating function $MP(z) = \sum_{n\ge0} MP_n\, z^n$ satisfies the functional equation

$$z(1-3z)MP^2(z) + (1-3z)MP(z) - 1 = 0. \tag{8.1}$$

When we apply our method from Section 3, the Ansatz for the base step is

$$MP_1(z) = \frac{1}{z}\Omega^{2^\alpha}(z^4) + \sum_{k=0}^{\alpha+1} \frac{z^{2^k-1}}{(1-z)^{2^k}}. \tag{8.2}$$

Subsequently, everything runs through in the same way as in the proof of Theorem 6. Consequently, the generating function $MP(z)$ for Motzkin prefix numbers satisfies a completely analogous theorem.

If we now follow the line of argument in Section 5, then we obtain that $MP(z)$ admits the following representation modulo 8:

$$\begin{aligned} MP(z) = \frac{4E(z^4)\Omega(z^4)}{z} &+ \left(\frac{1}{z} + \frac{4z^7+2z^6+2z^4+2z^2+4z+2}{1-z^8}\right)\Omega(z^4) \\ &+ \frac{4E(z^8)}{z} + \left(\frac{6}{z} + \frac{4}{1-z^2}\right)E(z^4) \\ + \frac{\begin{matrix} 6z^{15}+z^{14}+z^{12}+4z^{11}+5z^{10}+6z^9+z^8 \\ +6z^7+z^6+4z^5+z^4+4z^3+5z^2+2z+1 \end{matrix}}{1-z^{16}} & \quad \text{modulo } 8. \end{aligned} \tag{8.3}$$

Coefficient extraction using Lemmas 7–10 leads to the following theorem generalising [3, Cor. 3.2].

Theorem 14. *Let n be a positive integer with binary expansion*

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + \cdots .$$

The Motzkin prefix numbers MP_n satisfy the following congruences modulo 8:

$$MP_n \equiv_8 \begin{cases} 2s_2^2(n)+4e_2(n)+1, & \text{if } n \equiv 0 \pmod{16}, \\ 4s_2(n)+6, & \text{if } n \equiv 1 \pmod{16}, \\ 6s_2^2(n)+4e_2(n)+7, & \text{if } n \equiv 2 \pmod{16}, \\ 2s_2^2(n)+4e_2(n)+1, & \text{if } n \equiv 3 \pmod{16}, \\ 2s_2^2(n)+4e_2(n)+1, & \text{if } n \equiv 4 \pmod{16}, \\ 0, & \text{if } n \equiv 5 \pmod{16}, \\ 6s_2^2(n)+4e_2(n)+7, & \text{if } n \equiv 6 \pmod{16}, \\ 4s_2(n)+2n_4+4n_4s_2(n)+2, & \text{if } n \equiv 7 \pmod{16}, \\ 2s_2^2(n)+4e_2(n)+1, & \text{if } n \equiv 8 \pmod{16}, \\ 4s_2(n)+6, & \text{if } n \equiv 9 \pmod{16}, \\ 6s_2^2(n)+4e_2(n)+7, & \text{if } n \equiv 10 \pmod{16}, \\ 6s_2^2(n)+4e_2(n)+7, & \text{if } n \equiv 11 \pmod{16}, \\ 2s_2^2(n)+4e_2(n)+1, & \text{if } n \equiv 12 \pmod{16}, \\ 0, & \text{if } n \equiv 13 \pmod{16}, \\ 6s_2^2(n)+4e_2(n)+7, & \text{if } n \equiv 14 \pmod{16}, \\ 2s_2^2(n)+4e_2(n)+6n_{K+1}+4n_{K+1}s_2(n)+1, & \\ & \text{if } n \equiv 15 \pmod{16} \text{ and } K \text{ is even}, \\ 4s_2(n)+2n_{K+1}+4n_{K+1}s_2(n)+2, & \\ & \text{if } n \equiv 15 \pmod{16} \text{ and } K \text{ is odd}, \end{cases}$$

where $s_2(n)$, $e_2(n)$, and K are defined as in Theorem 11.

8.2. **Riordan numbers modulo 8.** Let R_n be the n-th *Riordan number*, that is, the number of lattice paths from $(0,0)$ to $(n,0)$ consisting of steps taken from the set $\{(1,0),(1,1),(1,-1)\}$ never running below the x-axis, and where steps $(1,0)$ are not allowed on the x-axis. It is well-known (cf. e.g. [8, Sec. 9]) that the generating function

$R(z)=\sum_{n\ge0} R_n\, z^n$ satisfies the functional equation

$$z(1+z)R^2(z)-(z+1)R(z)+1=0. \tag{8.4}$$

When we apply our method from Section 3, the Ansatz for the base step is the same as the one in the case of Motzkin prefix numbers, that is, the right-hand side of (8.2). Subsequently, everything runs through in the same way as in the proof of Theorem 6. Consequently, the generating function $R(z)$ for Riordan numbers satisfies a completely analogous theorem.

If we now follow the line of argument in Section 5, then we obtain that $R(z)$ admits the following representation modulo 8:

$$\begin{aligned} R(z)=\frac{4E(z^4)\Omega(z^4)}{z}&+\left(\frac{7}{z}+\frac{2z^6+4z^5+2z^4+4z^3+2z^2+2}{1-z^8}\right)\Omega(z^4)\\ &+\frac{4E(z^8)}{z}+\left(\frac{2}{z}+\frac{4}{1-z^2}\right)E(z^4)\\ +\frac{\begin{matrix}5z^{14}+2z^{13}+z^{12}+2z^{11}+z^{10}+4z^9+z^8\\ \qquad\qquad +5z^6+6z^5+z^4+2z^3+z^2+1\end{matrix}}{1-z^{16}}&\quad\text{modulo } 8. \end{aligned}\tag{8.5}$$

Coefficient extraction using Lemmas 7–10 leads to the following theorem generalising [3, Cor. 3.3].

Theorem 15. *Let n be a positive integer with binary expansion*

$$n=n_0+n_1\cdot 2+n_2\cdot 2^2+\cdots.$$

The Riordan numbers R_n satisfy the following congruences modulo 8:

$$R_n\equiv_8\begin{cases} 2s_2^2(n)+4e_2(n)+1, & \text{if } n\equiv 0 \pmod{16},\\ 0, & \text{if } n\equiv 1 \pmod{16},\\ 6s_2^2(n)+4e_2(n)+3, & \text{if } n\equiv 2 \pmod{16},\\ 2s_2^2(n)+4e_2(n)+5, & \text{if } n\equiv 3 \pmod{16},\\ 2s_2^2(n)+4e_2(n)+1, & \text{if } n\equiv 4 \pmod{16},\\ 4s_2(n)+6, & \text{if } n\equiv 5 \pmod{16},\\ 6s_2^2(n)+4e_2(n)+3, & \text{if } n\equiv 6 \pmod{16},\\ 6n_4+4n_4s_2(n)+4, & \text{if } n\equiv 7 \pmod{16},\\ 2s_2^2(n)+4e_2(n)+1, & \text{if } n\equiv 8 \pmod{16},\\ 0, & \text{if } n\equiv 9 \pmod{16},\\ 6s_2^2(n)+4e_2(n)+3, & \text{if } n\equiv 10 \pmod{16},\\ 6s_2^2(n)+4e_2(n)+7, & \text{if } n\equiv 11 \pmod{16},\\ 2s_2^2(n)+4e_2(n)+1, & \text{if } n\equiv 12 \pmod{16},\\ 4s_2(n)+6, & \text{if } n\equiv 13 \pmod{16},\\ 6s_2^2(n)+4e_2(n)+3, & \text{if } n\equiv 14 \pmod{16},\\ 2s_2^2(n)+4e_2(n)+2n_{K+1}+4n_{K+1}s_2(n)+5, & \\ & \text{if } n\equiv 15 \pmod{16} \text{ and } K \text{ is even},\\ 6n_{K+1}+4n_{K+1}s_2(n)+4, & \text{if } n\equiv 15 \pmod{16} \text{ and } K \text{ is odd}, \end{cases}$$

where $s_2(n)$, $e_2(n)$, and K are defined as in Theorem 11.

8.3. **Hex tree numbers modulo 8.** Let H_n be the n-th *hex tree number*, that is, the number of planar rooted trees where each vertex may have a left, a middle, or a right descendant, but never a left *and* middle descendant, and never a middle *and* right descendant. It is well-known (and easy to see) that the generating function $H(z) = \sum_{n\ge0} H_n\, z^n$ satisfies the functional equation

$$z^2H^2(z) + (3z-1)H(z) + 1 = 0. \tag{8.6}$$

When we apply our method from Section 3, the Ansatz for the base step is

$$H_1(z) = \frac{1-z}{z^2}\Omega^{2^\alpha}(z^4) + \sum_{k=1}^{\alpha+1} \frac{z^{2^k-2}}{(1-z)^{2^k-1}}.$$

Subsequently, everything runs through in the same way as in the proof of Theorem 6. Consequently, the generating function $H(z)$ for hex tree numbers satisfies a completely analogous theorem.

If we now follow the line of argument in Section 5, then we obtain that $H(z)$ admits the following representation modulo 8:

$$\begin{aligned} H(z) = {}&\frac{4E(z^4)\Omega(z^4)(z+1)}{z^2}\\ &+\left(\frac{7}{z^2}+\frac{3}{z}+\frac{6z^7+2z^6+2z^5+6z^4+2z^3+6z^2+6z+2}{1-z^8}\right)\Omega(z^4)\\ &\qquad+\frac{4E(z^8)(z+1)}{z^2}+\left(\frac{2}{z^2}+\frac{2}{z}+\frac{4}{1-z}\right)E(z^4)\\ &+\frac{\begin{matrix}3z^{15}+5z^{14}+5z^{13}+3z^{12}+z^{11}+3z^{10}+7z^9+5z^8\\ \qquad +3z^7+5z^6+z^5+7z^4+z^3+3z^2+3z+1\end{matrix}}{1-z^{16}} \quad \text{modulo } 8. \end{aligned} \tag{8.7}$$

Coefficient extraction using Lemmas 7–10 leads to the following theorem generalising [3, Cor. 3.4].

Theorem 16. *Let n be a positive integer with binary expansion*

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + \cdots .$$

The hex tree numbers H_n satisfy the following congruences modulo 8:

$$H_n \equiv_8 \begin{cases} 2s_2^2(n) + 4e_2(n) + 1, & \text{if } n \equiv 0 \pmod{16},\\ 2s_2^2(n) + 4e_2(n) + 1, & \text{if } n \equiv 1 \pmod{16},\\ 4s_2(n) + 6, & \text{if } n \equiv 2 \pmod{16},\\ 4, & \text{if } n \equiv 3 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 3, & \text{if } n \equiv 4 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 7, & \text{if } n \equiv 5 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 2n_4 + 4n_4 s_2(n) + 7, & \text{if } n \equiv 6 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 6n_4 + 4n_4\, s_2(n) + 7, & \text{if } n \equiv 7 \pmod{16},\\ 2s_2^2(n) + 4e_2(n) + 1, & \text{if } n \equiv 8 \pmod{16},\\ 2s_2^2(n) + 4e_2(n) + 1, & \text{if } n \equiv 9 \pmod{16},\\ 4, & \text{if } n \equiv 10 \pmod{16},\\ 4s_2(n) + 6, & \text{if } n \equiv 11 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 3, & \text{if } n \equiv 12 \pmod{16},\\ 6s_2^2(n) + 4e_2(n) + 7, & \text{if } n \equiv 13 \pmod{16},\\ 4s_2(n) + 6n_{K+1} + 4n_{K+1}s_2(n) + 6, & \text{if } n \equiv 14 \pmod{16} \text{ and } K \text{ is even},\\ 6s_2^2(n) + 4e_2(n) + 2n_{K+1} + 4n_{K+1}s_2(n) + 7, & \\ & \text{if } n \equiv 14 \pmod{16} \text{ and } K \text{ is odd},\\ 2n_{K+1} + 4n_{K+1}s_2(n) + 4, & \text{if } n \equiv 15 \pmod{16} \text{ and } K \text{ is even},\\ 6s_2^2(n) + 4e_2(n) + 6n_{K+1} + 4n_{K+1}s_2(n) + 7, & \\ & \text{if } n \equiv 15 \pmod{16} \text{ and } K \text{ is odd}, \end{cases}$$

where $s_2(n)$, $e_2(n)$, and K are defined as in Theorem 11.

Inspection of the above sixteen cases reveals the interesting fact that hex tree numbers are never divisible by 8 (a fact that is also true for Motzkin numbers).

8.4. **Central trinomial coefficients modulo** 8. Let T_n be the n-th *central trinomial coefficient*, that is, the coefficient of t^n in $(1 + t + t^2)^n$. Already Euler knew that the generating function $T(z) = \sum_{n\ge0} T_n\, z^n$ equals

$$T(z) = (1 - 2z - 3z^2)^{-1/2} \tag{8.8}$$

(cf. [11, solution to Exercise 6.42]).

Here we proceed differently in order to express $T(z)$ in terms of our basic series $\Omega(z^4)$ (and the error series $E(z^4)$). We are forced to do so since our method from Section 3 fails.[3] Instead, we compare (1.1) and (8.8) to see that[4]

$$T(z)=\frac{1-z-2z^2M(z)}{1-2z-3z^3}. \tag{8.9}$$

Relation (8.9) would allow us to establish a complete analogue of Theorem 6 for the generating function $T(z)$ for central trinomial coefficients. In order to determine these numbers modulo 8, we substitute (5.4) in the above relation. Then some simplification eventually leads to

$$\begin{aligned}T(z)=\frac{6z^3+6z^2+2z+2}{1-z^4}\Omega(z^4)+\frac{4E(z^4)}{1-z}\\+\frac{3z^7+7z^6+z^5+z^4+7z^3+3z^2+z+1}{1-z^8}\quad\text{modulo } 8.\end{aligned} \tag{8.10}$$

Coefficient extraction using Lemmas 8 and 9 leads to the following theorem for central trinomial coefficients modulo 8.

Theorem 17. *Let n be a positive integer with binary expansion*

$$n=n_0+n_1\cdot 2+n_2\cdot 2^2+\cdots .$$

Modulo 8, the central trinomial coefficients T_n satisfy the following congruences:

$$T_n\equiv_8\begin{cases}2s_2^2(n)+4e_2(n)+1, & \text{if } n\equiv 0 \pmod 2,\\ 6s_2^2(n)+4e_2(n)+3, & \text{if } n\equiv 1 \pmod 2,\end{cases}$$

where $s_2(n)$ and $e_2(n)$ are defined as in Theorem 11.

Note

The result in Theorem 11 has in the meantime also been obtained — in slightly different form and using a different approach — by Wang and Xin in "A Classification of Motzkin Numbers Modulo 8" [Electron. J. Combin. **25**(1) (2018), Article P1.54, 15 pp.].

Acknowledgement

The authors are indebted to an anonymous referee for clarifying the scope of the automaton method of Rowland and Yassawi in [10].

[3]The base step solution would be the one with $a_0(z)=1/(1-z)$ and $a_{2^\alpha}(z)=0$. Subsequently, the iteration step modulo 4 would not succeed, however. We believe that the reason for this phenomenon might be that the minimal polynomial for Ω (in the sense of [7, 8, 9]) is of degree less than 4.

[4]A similar approach would also have been possible for the Motzkin prefix and the Riordan numbers since their generating functions satisfy relations with the generating function $M(z)$ for Motzkin numbers analogous to (8.9). However, no such relation exists between the generating function for hex tree numbers and $M(z)$.

References

[1] G. E. Andrews, *The Theory of Partitions*, Encyclopedia of Math. and its Applications, Vol. 2, Addison–Wesley, Reading, 1976; reprinted by Cambridge University Press, Cambridge, 1998.

[2] F. Bergeron and C. Reutenauer, Combinatorial resolution of systems of differential equations III: a special class of differentially algebraic series, *Europ. J. Combin.* **11** (1990), 501–512.

[3] E. Deutsch and B. E. Sagan, Congruences for Catalan and Motzkin numbers and related sequences, *J. Number Theory* **117** (2006), 191–215.

[4] S.-P. Eu, S.-C. Liu, and Y.-N. Yeh, Catalan and Motzkin numbers modulo 4 and 8, *Europ. J. Combin.* **29** (2008), 1449–1466.

[5] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, Cambridge, 2009.

[6] D. Gouyou-Beauchamps and X. Viennot, Equivalence of the two-dimensional directed animal problem to a one-dimensional path problem, *Adv. Appl. Math.* **9** (1988), 334–357.

[7] M. Kauers, C. Krattenthaler, and T. W. Müller, A method for determining the mod-2^k behaviour of recursive sequences, with applications to subgroup counting, *Electron. J. Combin.* **18**(2) (2012), Article P37, 83 pp.

[8] C. Krattenthaler and T. W. Müller, A method for determining the mod-3^k behaviour of recursive sequences, preprint; `ar`χ`iv:1308.2856`.

[9] C. Krattenthaler and T. W. Müller, A method for determining the mod-p^k behaviour of recursive sequences, preprint; `ar`χ`iv:1508.02580`.

[10] E. Rowland and R. Yassawi, *Automatic congruences for diagonals of rational functions*, *J. Théorie Nombres Bordeaux* **27** (2015), 245–288.

[11] R. P. Stanley, *Enumerative Combinatorics*, vol. 2, Cambridge University Press, Cambridge, 1999.

†*Fakultät für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, A-1090 Vienna, Austria. WWW: `http://www.mat.univie.ac.at/~kratt`.

*School of Mathematical Sciences, Queen Mary & Westfield College, University of London, Mile End Road, London E1 4NS, United Kingdom.