A classification of Motzkin numbers modulo 8

Ying Wang
School of Mathematical Sciences
Capital Normal University
Beijing 100048, PR China
wangying.cnu@gmail.com

Guoce Xin
School of Mathematical Sciences
Capital Normal University
Beijing 100048, PR China
guoce.xin@gmail.com

Submitted: Jun 10, 2017; Accepted: Dec 9, 2017; Published: Mar 16, 2018
Mathematics Subject Classifications: 05A10, 11B50

Abstract

The well-known Motzkin numbers were conjectured by Deutsch and Sagan to be nonzero modulo 8. The conjecture was first proved by Sen-Peng Eu, Shu-chung Liu and Yeong-Nan Yeh by using the factorial representation of the Catalan numbers. We present a short proof by finding a recursive formula for Motzkin numbers modulo 8. Moreover, such a recursion leads to a full classification of Motzkin numbers modulo 8.

Keywords: Motzkin numbers, congruence classes

1 Introduction

Much work has been done in calculating the congruences of various combinatorial numbers modulo a prime power $p^r$. We begin by introduce some notations. We will use the $p$-adic notations $[n]_p = ⟨n_d n_{d-1} \cdots n_0⟩_p$ to denote the sequence of digits representing $n$ in base $p$ [15]. The $p$-adic order or $p$-adic valuation $\omega_p(n)$ of $n$ is defined by

$$\omega_p(n) = \max\{t \in \mathbb{N} : p^t | n\}.$$ 

In words, it is the highest power of $p$ dividing $n$, or equivalently, the number of 0’s to the right of the rightmost nonzero digit in $[n]_p$. The value $\omega_p(n)$ indicates the divisibility by powers of $p$, which can be found in many previous studies [5].

Many results have been established for the binomial coefficients. The most famous as well as age-old one is the Pascal’s fractal which is formed by the parities of the binomial coefficients $\binom{n}{k}$ [20]. Pascal’s triangle also has versions modulo 4 and 8 [3, 10]. The behavior of Pascal’s triangle modulo higher powers of $p$ is more complicated. Some rules

*This work is partially supported by National Natural Science Foundation of China (11171231).
for this behavior are discussed by Granville [9]. Kummer computed the $p$-adic order of \( \binom{m+n}{m} \) [13], by counting the number of carries that occur when \([m]_p\) and \([n]_p\) are added. The elegant result of Lucas [15] states that \( \binom{n}{m} \equiv p \prod_i \binom{n_i}{k_i} \) where \( n_i \) and \( k_i \) come from \([n]_p\) and \([k]_p\), and \( \equiv_p \) denotes the congruence class modulo \( p \). A generalization of Lucas’ theorem for a prime power was established by Davis and Webb [2].

The most useful combinatorial numbers other than the binomial coefficients are the well-known Catalan numbers

\[
C_n = \frac{1}{n+1} \binom{2n}{n} = \frac{(2n)!}{n!(n+1)!}, \quad n \in \mathbb{N}.
\]

They have more than 200 combinatorial interpretations, as collected by Stanley in [18]. The congruence class of \( C_n \) modulo \( 2^r \) was studied in [6, 11, 14, 21]. Several other combinatorial numbers have been studied for their congruences, for example, Apéry numbers [8, 16], Central Delannoy numbers [7] and weighted Catalan numbers [17].

In this paper we will focus on the well-known Motzkin numbers

\[
M(n) = M_n = \sum_{k \geq 0} \binom{n}{2k} C_k, \quad n \in \mathbb{N}.
\] (1)

Their congruences were only studied very recently. Klazar and Luca proved that the Motzkin numbers are never periodic modulo any prime number [12]. Deutsch and Sagan [4] studied the congruences of \( M_n \) modulo 2, 3 and 5 and made the following two conjectures.

**Conjecture 1** ([4]). We have \( M_n \equiv_4 0 \) if and only if \( n = (4i + 1)4^{j+1} - 1 \) or \( n = (4i + 3)4^{j+1} - 2 \), where \( i \) and \( j \) are nonnegative integers.

**Conjecture 2** ([4]). The Motzkin numbers are never congruent to 0 modulo 8.

The two conjectures were first proved by Eu-Liu-Yeh in [6]. They first derived the congruence class of the Catalan numbers \( C_n \) modulo 8 by using their factorial representations. Then they proved Conjecture 1 by careful analyzing formula (1) modulo 8. Finally they proved Conjecture 2 by confirming that \( M(n) \equiv_8 4 \) when \( n \) belongs to the two cases in Conjecture 1.

Our main result is the following explicit formula for \( M_n \) modulo 8, from which Conjectures 1 and 2 clearly follow.

**Theorem 3.** The congruence class of \( M(n) \) modulo 8 can be characterized as follows:

\[
M(4s) \equiv_8 \begin{cases} 
1 - 4Z(\alpha) - 2\chi(\alpha \equiv_2 1) + 4\alpha, & s = 2\alpha, \\
1 - 4Z(\alpha) - 2\chi(\alpha \equiv_2 1), & s = 2\alpha + 1.
\end{cases}
\]

\[
M(4s + 1) \equiv_8 \begin{cases} 
1 - 4Z(\alpha) - 2\chi(\alpha \equiv_2 1) + 4\alpha, & s = 2\alpha, \\
1 - 4Z(\alpha) - 2\chi(\alpha \equiv_2 1) + 4, & s = 2\alpha + 1.
\end{cases}
\]
Here \( \chi(S) \) equals 1 if the statement \( S \) is true and equals 0 if otherwise, \( \|\alpha\| \) is the sum of the digits of \([\alpha]_2\), and \( Z(\alpha) \) is the number of zero runs of \( \alpha \) as described later in Proposition 11.

Our approach is along the line of [21], by using the following recursive formula:

\[
C_{n+1} = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} 2^{n-2i} C_i.
\]

This formula can be easily proved by using Zeilberger’s creative telescoping method [22], or by two different combinatorial interpretations of \( C_n \) (see [21]). By combining the above formula with (1), we derive the following recursive formulas for \( M(\cdot) \).

\[
M(2k + 2) - M(2k) \equiv_8 (-1)^k M(k) + f(k),
\]
\[
f(k) = 4 \left( \binom{k+1}{2} - (-1)^k k \right) M(k-1) - 4 \binom{k}{2} M(k-2);\]
\[
M(2k + 1) \equiv_8 (2k + 1) M(2k) + g(k),
\]
\[
g(k) = -2 \left( \binom{2k+1}{2} \right) M(2k-1) + 4 \binom{2k+1}{3} M(2k-2).
\]

By using these recursive formulas, we give a simple way to compute the congruences of \( M(n) \) modulo 2, 4, 8.

The paper is organized as follow. In Section 2, we derive the recurrence formulas of \( M_n \), which are the starting point of our approach. We also introduce basic tools for further calculations. In Section 3, we compute the congruence classes of Motzkin numbers modulo 2 and 4. Finally, we compute the congruence classes of Motzkin numbers modulo 8 in Section 4.

2 Weighted Motzkin paths and the recursion

Let \( F(x; u) = \sum_{n \geq 0} M_u(n) x^n \) be the unique power series defined by the functional equation

\[
F(x; u) = \frac{1}{1 - ux - x^2 F(x; u)}.
\]
Then $F(x; u)$ is the generating function of weighted Motzkin paths (see, e.g. [19]). That is, $M_u(n)$ counts weighted lattice paths from $(0, 0)$ to $(n, 0)$ that never go below the horizontal axis and use only steps $U = (1, 1)$ $H = (1, 0)$, or $D = (1, -1)$ and weights $1, u, 1$ respectively.

The well-known Motzkin number $M(n)$ is our $M_1(n)$, and the Catalan number $C_n$ is our $M_0(2n)$. We also have $C_{n+1} = M_2(n)$, which is written as

$$M_0(2n) = M_2(n - 1), \quad \text{for } n \geq 1. \quad (4)$$

**Lemma 4.** For any constants $u$ and $v$, we have

$$M_{u+v}(n) = \sum_{i=0}^{n} \binom{n}{i} v^i M_u(n - i), \quad (5)$$

$$M_u(2k + 1) = \sum_{i=1}^{n} \binom{2k + 1}{i} (-2)^{i-1} u^i M_u(2k + 1 - i). \quad (6)$$

**Proof.** Equation (5) is routine. For (6), we need the easy fact $M_{-u}(n) = (-1)^n M_u(n)$. By setting $v = -2u$ in (5), we obtain

$$M_{-u}(n) = M_u(n) + \sum_{i=1}^{n} \binom{n}{i} (-2u)^i M_u(n - i).$$

Thus for $n = 2k + 1$, we obtain

$$M_u(2k + 1) = \sum_{i=1}^{n} \binom{2k + 1}{i} (-2)^{i-1} u^i M_u(2k + 1 - i).$$

This is equation (6). 

**Theorem 5.** We have the recursion (2) and (3) with initial condition $M(0) = 1$.

**Proof.** Setting $u = 1$ in (6) and simplifying gives

$$M(2k + 1) \equiv_8 (2k + 1)M(2k) - 2 \left(\frac{2k + 1}{2}\right) M(2k - 1) + 4 \left(\frac{2k + 1}{3}\right) M(2k - 2).$$

This is (3). Note that no recursion for $M(2k)$ can be obtained in this way.

For (2), we start with

$$M(2k) = \sum_{i=0}^{k} \binom{2k}{2i} C_{k-i}$$

$$= \sum_{i=0}^{k} \sum_{j=0}^{i} 2^{2j} \binom{k}{2j} \binom{k-2j}{i-j} C_{k-i},$$

THE ELECTRONIC JOURNAL OF COMBINATORICS 25(1) (2018), #P1.54

4
which can be easily proved using Zeilberger’s creative telescoping method [22]. When reduced to modulo 8, this gives

\[ M(2k) \equiv 8 \sum_{i=0}^{k} \binom{k}{i} C_{k-i} + 4 \binom{k}{2} \sum_{i=1}^{k-1} \binom{k-2}{i-1} C_{k-i} \]

\[ \equiv 8 \left( 1 + \sum_{i=0}^{k-1} \left( \sum_{j=1}^{i} \binom{k-j}{i-j+1} \right) M_2(k-i-1) + 4 \binom{k}{2} \sum_{i'=0}^{k-2} \binom{k-2}{i'} M_2(k-2-i') \right) \]

\[ \equiv 8 \left( 1 + \sum_{j=1}^{k-1} \sum_{i=j}^{k-1} \binom{k-j}{i-j+1} M_2((k-j)-(i-j+1)) + 4 \binom{k}{2} M_3(k-2) \right) \]

\[ \equiv 8 \left( 1 + \sum_{j=1}^{k-1} M_3(k-j) + 4 \binom{k}{2} M_3(k-2) \right). \]

(We remark that the computation modulo 2^r when r \geq 4 becomes complicated.) Thus,

\[ M(2k+2) - M(2k) \equiv 8 M_3(k) + 4 \binom{k+1}{2} M_3(k-1) - 4 \binom{k}{2} M_3(k-2) \]

\[ \equiv 8 M_{-1}(k) + 4 \binom{k}{1} M_{-1}(k-1) + 4 \binom{k+1}{2} M(k-1) - 4 \binom{k}{2} M(k-2) \]

\[ \equiv 8 (-1)^k M(k) + 4 \left( \binom{k+1}{2} - (-1)^k \right) M(k-1) - 4 \binom{k}{2} M(k-2). \]

This is just equation (2). \qed

We derive explicit formulas of \( M(n) \mod 2^r \) successively for \( r = 1, 2, 3 \). The idea is based on the fact that

\[ 2^{r-r'} M(n) \mod 2^r = 2^{r-r'} (M(n) \mod 2^r), \quad \text{for } r' < r. \]

This fact will be frequently used without mentioning.

**Lemma 6.** We keep the notations from Theorem 5. Assume that we have obtained explicit formulas for \( M(n) \mod 2^{r-1} \). Then there are explicit formulas for \( f(k) \) and \( g(k) \). Moreover, the recursion is reduced as follows.

\[ M(2k+1) \equiv 8 (2k+1) M(2k) + g(k), \quad (7) \]

\[ M(4s) \equiv 2^{r} M(0) + \sum_{j=2}^{2s-1} f(j) - \sum_{j=1}^{s-1} (2j M(2j) + g(j)), \quad (8) \]

\[ M(4s+2) \equiv 2^{r} M(2\beta-2) + \sum_{i=0}^{a} \left( M(\beta 2^{i+2} - 4) + f(\beta 2^{i+1} - 2) \right), \quad (9) \]

where in (9), \( s + 1 = \beta 2^a \) for some odd number \( \beta \) and \( a \geq 0 \).
Proof. By (7), we can eliminate those $M(2k + 1)$ so that our formulas only involve $f(k), g(k)$ and $M(2k)$. We have to split by cases $k = 2s$ and $k = 2s + 1$ in (2):

\[
M(4s + 4) - M(4s + 2) \equiv 2r - M(2s + 1) + f(2s + 1)
\]
\[
\equiv 2r - (2s + 1)M(2s) - g(s) + f(2s + 1),
\]
\[
M(4s + 2) - M(4s) \equiv 2r - M(2s) + f(2s) \equiv 2r - M(2s) + f(2s).
\]

Taking the sum of the above two equations gives the following recursion:

\[
M(4s + 4) - M(4s) \equiv 2r - 2sM(2s) - g(s) + f(2s) + f(2s + 1).
\]

(Note that we have explicit formulas of $-2sM(2s) \mod 2^r$ by the induction hypothesis.) This is equivalent to (8).

Next for $M(4s + 2)$ we rewrite as follows:

\[
M(4(s + 1) - 2) - M(4s) \equiv 2r - M(2(s + 1) - 2) + f(2s).
\]

If $s = \beta 2^a - 1$ with $\beta$ odd and $a \geq 0$, then the above equation can be rewritten as

\[
M(\beta 2^{a+2} - 2) - M(\beta 2^{a+1} - 2) \equiv 2r - M(\beta 2^{a+2} - 4) + f(\beta 2^{a+1} - 2).
\]

This is equivalent to (9).

We remark that (8') and (9') are easier to use than (8) and (9).

3 Motzkin numbers modulo 2, 4

Recall that $\omega_2(n) = a$ if $n = (2\alpha + 1)2^a$. Note that $\omega_2(0)$ is not defined. The following properties are easy to check and will be frequently used without mentioning.

Lemma 7. For nonnegative integer $\alpha$ we have

\[
\omega_2(2\alpha + 1) = 0, \quad \omega_2(2\alpha) = \omega_2(\alpha) + 1, \quad \alpha \omega_2(\alpha) \equiv 2 \ 0;
\]
\[
\omega_2(\alpha!) = \sum_{i=1}^{\alpha} \omega_2(i), \quad \omega_2((2\alpha + 1)!) = \omega_2((2\alpha)!)) = \omega_2(\alpha!) + \alpha.
\]

Proof. The first, second and fourth formulas follow easily by definition. The third formula follows from the first two formulas by discussing the parity of $\alpha$. Finally,

\[
\omega_2((2\alpha + 1)!) = \omega_2((2\alpha)!) = \omega_2((2\alpha)!!)) = \omega_2(\alpha!) + \alpha,
\]

where in the second equality, we removed all the odd factors to get $(2\alpha)!! = 2^a\alpha!$. \qed
3.1 Motzkin numbers modulo 2

**Proposition 8.** We have

\[ M(2k + 1) \equiv_2 M(2k) \equiv_2 \omega_2(2k + 2). \]

In particular \( M(4s) \equiv_2 M(4s + 1) \equiv_2 1. \)

**Proof.** We apply Theorem 5 and Lemma 6 and follow the notations there. Clearly, we have \( f(k) \equiv_2 0 \) and \( g(k) \equiv_2 0. \) Thus we have

\[ M(4s) \equiv_2 M(0) = 1 = \omega_2(4s + 2), \]
\[ M(4s + 2) \equiv_2 M(2\beta - 2) + \sum_{i=0}^{\alpha} \left( M(2\beta^i - 4) \right) = a + 2 = \omega_2(4s + 4), \]

where in the second equation, \( s + 1 = \beta 2^a \) for some odd number \( \beta \) and \( a \geq 0. \) The proposition then follows. \( \square \)

3.2 Motzkin numbers modulo 4

**Lemma 9.** We have the following characterization of Motzkin numbers modulo 4.

\[ M(4s) \equiv_4 1 + 2\omega_2(s!) \equiv_4 1 + 2L(s) + 2s, \]
\[ M(4s + 1) \equiv_4 M(4s), \]
\[ M(4s + 2) \equiv_4 \begin{cases} 2\alpha + 2, & s = (2\alpha + 1)2^{2\alpha} - 1, a \geq 0, \\ 2\alpha + 2L(\alpha) + 3, & s = (2\alpha + 1)2^{2\alpha+1} - 1, a \geq 0. \end{cases} \]
\[ M(4s + 3) \equiv_4 -M(4s + 2) + 2, \]

where \( L(r) = \sum_{i=1}^{r-1} M(2i). \)

Consequently, \( M(n) \equiv_4 0 \) if and only if \( n = (4i + 1)4^{i+1} - 1 \) or \( n = (4i + 3)4^{i+1} - 2 \) for some nonnegative integers \( i \) and \( j. \) That is, Conjecture 1 holds true.

**Proof.** We first show that the second part follows from the first part. Clearly, \( M(n) \equiv_4 0 \) if and only if either i) \( M(n) = M(4r + 2) \equiv_4 2\alpha + 2 \equiv_4 0 \) for \( r = (2\alpha + 1)4^a - 1. \) Hence, \( \alpha = 2i + 1 \) for some \( i \) and \( n = (4i + 3)4^{i+1} - 2; \) Or ii) \( M(n) = M(4r + 3) \equiv_4 -M(4r + 2) + 2 \equiv_4 2\alpha \equiv_4 0 \) for \( r = (2\alpha + 1)4^a - 1. \) Hence, \( \alpha = 2i \) for some \( i \) and \( n = (4i + 1)4^{i+1} - 1. \)

Now we prove the first part by Theorem 5 and Lemma 6. First, we have

\[ f(k) \equiv_4 0 \quad \text{and} \quad g(k) \equiv_4 -2k(2k + 1)M(2k - 1) \equiv_4 2k\omega_2(2k) \equiv_4 2k, \]

where we have used Proposition 8. Thus, the recurrence reduces to

\[ M(2k + 2) \equiv_4 M(2k) + (-1)^k M(k), \] (10)
\[ M(2k + 1) \equiv_4 (2k + 1)M(2k) + 2k. \] (11)
Clearly, the odd case reduces to the even case by (11).

For $M(4s)$ we have

$$M(4s + 4) - M(4s) \equiv_4 -M(2s + 1) + M(2s) \equiv_4 -2sM(2s) - 2s$$

$$\equiv_4 2\chi(s = 2\alpha + 1)(1 + \omega_2(\alpha + 1) + 1) \equiv_4 2\omega_2(s + 1),$$

which is equivalent to $M(4s) \equiv_4 1 + 2\omega_2(s!) \equiv_4 1 + 2L(s) + 2s$.

For $M(4s + 2)$, we write $s = \beta 2^a - 1$ for a unique odd number $\beta$. We have

$$M(4s + 2) \equiv_4 M(2\beta - 2) + \sum_{i=0}^{a} M(\beta 2^{i+2} - 4)$$

$$\equiv_4 M(2\beta - 2) + \sum_{i=0}^{a} (1 + 2L(\beta 2^i - 1) + 2(\beta 2^i - 1))$$

$$\equiv_4 \chi(\beta = 2\alpha + 1)1 + 2L(\alpha) + 2\alpha - (a + 1) + \sum_{i=0}^{a} (2i + 2L(\alpha) + 2^{i+1})$$

$$\equiv_4 2(a + 2)L(\alpha) + 2\alpha - a + a(a + 1) + 2$$

$$\equiv_4 2(a + 2)L(\alpha) + 2\alpha + a^2 - 2$$

$$\equiv_4 \begin{cases} 2\alpha + 2, & a \text{ is even,} \\ 2\alpha + 2L(\alpha) + 3, & a \text{ is odd.} \end{cases}$$

This completes the proof. $\square$

Indeed since $L(s)$ appears in computations modulo 8, we summarize its properties as follows.

**Lemma 10.** Let $L(s) = \sum_{i=0}^{s-1} M(2i)$, with $L(0) = 0$. Then

$$L(2s) \equiv_2 L(s), \quad L(2s + 1) \equiv_2 1 + L(s), \quad L(s) = h_2(s!) + s,$$

$$L(2s) \equiv_4 1 - (-1)^s + L(s), \quad L(2s + 1) \equiv_4 1 - L(s).$$

**Proof.** The modulo 2 result is obvious since $L(s) \equiv_2 \sum_{i=0}^{s-1} \omega_2(2i + 2) = \omega_2(s!) + s$.

For the modulo 4 result, we have, by definition,

$$L(2s) \equiv_4 \sum_{i=0}^{2s-1} M(2i) = \sum_{i=0}^{s-1} (M(4i + 2) + M(4i))$$

(by (10)) $\equiv_4 \sum_{i=0}^{s-1} (2M(4i) + M(2i))$

$$\equiv_4 \sum_{i=0}^{s-1} (2 + M(2i))$$

$$\equiv_4 2s + L(s)$$
\[ \equiv_4 1 - (-1)^s + L(s). \]

By the above formula and Lemma 9, we have

\[ L(2s + 1) = L(2s) + M(4s) = 2s + L(s) + 1 + 2s = 1 - L(s). \]

This completes the proof. \( \Box \)

Let \([n]_2 = n_kn_{k-1} \cdots n_1n_0\) be the binary expansion of \(n \geq 1\). Then \(n = n_k2^k + \cdots + n_1 \cdot 2 + n_0\). Denote by \(\|n\| = n_k + \cdots + n_1 + n_0\), the sum of the binary digits of \(n\). A 0-run of \([n]_2\) is a maximal 0-subword \(n_in_{i+1} \cdots n_j\) for some \(0 \leq i < j \leq k\), such that \(n_{j+1} = 1\) and \(n_{i-1} \neq 0\) (including the case \(i = 0\)). Denote by \(Z(n)\) the number of 0-runs of \([n]_2\).

We have the following explicit result.

**Proposition 11.** We have

\[ L(n) \equiv_2 \|n\|, \quad \text{and} \quad L(n) \equiv_4 2Z(n) + \chi(\|n\| \equiv_2 1). \]

**Proof.** The modulo 2 case is straightforward by Lemma 10.

For the modulo 4 case, we proceed by induction on \(n\). The proposition clearly holds for the base case \(n = 1\). Assume it holds for all numbers smaller than \(n\). We show that it holds for \(n\) by considering the following two cases.

Case 1: If \(n = 2s + 1\), then \([n]_2\) is obtained from \([s]_2\) by adding a 1 at the end. By Lemma 10 and the induction hypothesis for \(s\), we have

\[ L(2s + 1) \equiv_4 1 - L(s) \equiv_4 1 - 2Z(s) - \chi(\|s\| \equiv_2 1) \equiv_4 2Z(s) + 1 - \chi(\|s\| \equiv_2 1), \]

which clearly equals to \(2Z(n) + \chi(\|n\| \equiv_2 1)\).

Case 2: If \(n = 2s\), then \([n]_2\) is obtained from \([s]_2\) by adding a 0 at the end. i) If \(s\) is odd, then by Lemma 10 and the induction hypothesis for \(s\), we have

\[ L(2s) \equiv_4 1 - (-1)^s + L(s) = 2 + L(s) = 2(Z(s) + 1) + \chi(\|s\| \equiv_2 1), \]

which clearly equals to \(2Z(n) + \chi(\|n\| \equiv_2 1)\). ii) Similarly, if \(s\) is even, then

\[ L(2s) \equiv_4 1 - (-1)^s + L(s) = L(s) = 2Z(s) + \chi(\|s\| \equiv_2 1). \]

This also equals to \(2Z(n) + \chi(\|n\| \equiv_2 1)\). \( \Box \)

We remark that the sequence \(L(n) \mod 2\) turns out to be the Thue-Morse sequence. See [1] for a survey on the Thue-Morse sequence.
4 Motzkin numbers modulo 8

Lemma 12. The recursion from Theorem 5 reduces modulo 8 to

\[ M(2k + 2) - M(2k) \equiv_8 (-1)^k M(k) + f(k), \quad \text{where} \quad f(k) = 4\chi(k \equiv_4 3)\omega_2((k + 1)/2), \]

\[ M(2k + 1) \equiv_8 (2k + 1)M(2k) + g(k), \]

where \( g(k) = \chi(k = 2\alpha + 1)(4\alpha - 2M(4\alpha)). \)

Proof. By Theorem 5, we have

\[ f(k) \equiv_8 4\left(\binom{k + 1}{2} - (-1)^k k\right)M(k - 1) - 4\binom{k}{2} M(k - 2). \]

i) When \( k = 2\alpha \), we have

\[ f(2\alpha) \equiv_8 4(\alpha - 2\alpha)M(2\alpha - 1) - 4\alpha M(2\alpha - 2) \equiv_8 4\alpha \omega_2(2\alpha) \equiv_8 0. \]

ii) When \( k = 2\alpha + 1 \), we have

\[ f(2\alpha + 1) \equiv_8 4(\alpha + 1 + 2\alpha + 1)M(2\alpha) - 4\alpha M(2\alpha - 1) \equiv_8 4\alpha \omega_2(2\alpha + 2) - 4\alpha \omega_2(2\alpha) \equiv_8 4\chi(\alpha \equiv_2 1)\omega_2(\alpha + 1) \equiv_8 4\chi(k \equiv_4 3)\omega_2((k + 1)/2). \]

We also have

\[ g(k) \equiv_8 -2\binom{2k + 1}{2} M(2k - 1) + 4\binom{2k + 1}{3} M(2k - 2). \]

i) When \( k = 2\alpha \), we have

\[ g(2\alpha) \equiv_8 -4\alpha M(4\alpha - 1) \equiv_8 4\alpha \omega_2(4\alpha) \equiv_8 0. \]

ii) When \( k = 2\alpha + 1 \), we have

\[ g(2\alpha + 1) \equiv_8 -2(2\alpha + 3)M(4\alpha + 1) + 4M(4\alpha) \equiv_8 4\alpha M(4\alpha) - 2M(4\alpha) \equiv_8 4\alpha - 2M(4\alpha). \]

This completes the proof.

Now we are ready to prove Theorem 3, which, by Proposition 11, can be restated as Propositions 13 and 14 blow.

Proposition 13. We have

\[ M(4s) \equiv_8 \begin{cases} 1 - 2L(\alpha) + 4\alpha, & s = 2\alpha, \\ 1 - 2L(\alpha), & s = 2\alpha + 1. \end{cases} \]
Proof. We apply Lemmas 6 and 12 to obtain
\[ M(4s + 4) - M(4s) \equiv_{8} f(2s) + f(2s + 1) - 2sM(2s) - g(s) \]
\[ \equiv_{8} -2sM(2s) + \chi(s = 2\alpha + 1)(4\omega_2(2\alpha + 2) - 4\alpha + 2M(4\alpha)). \]
i) When \( s = 2\alpha \), we have
\[ M(4s + 4) - M(4s) \equiv_{8} -4\alpha M(4\alpha) \equiv_{8} 4\alpha \omega_2(4\alpha + 2) \equiv_{8} 4\alpha. \]
ii) When \( s = 2\alpha + 1 \), we have
\[ M(4s + 4) - M(4s) \equiv_{8} -2M(4\alpha + 2) \equiv_{8} -2M(4\alpha + 1) \]
where the last step is easily checked by considering the parity of \( \alpha \).

Finally, let \( M'(4s) \) be defined by the right hand side of (12). Then \( M'(0) = 1 \) and
\[ M'(8\alpha + 4) - M'(8\alpha) \equiv_{8} 4\alpha, \]
\[ M'(8\alpha + 8) - M'(8\alpha + 4) \equiv_{8} 1 - 2L(\alpha + 1) + 4(\alpha + 1) - 1 + 2L(\alpha) \]
\[ \equiv_{8} 4(\alpha + 1) - 2M(2\alpha). \]
Thus \( M(4s) = M'(4s) \) and the proposition follows.

The next results relies on Proposition 13.

Proposition 14. We have
\[
\begin{align*}
M(4s + 1) &\equiv_{8} \begin{cases} 
1 - 2L(\alpha) + 4\alpha, & s = 2\alpha, \\
1 - 2L(\alpha) + 4, & s = 2\alpha + 1.
\end{cases} \\
M(4s + 2) &\equiv_{8} \begin{cases} 
4, & s = (4\alpha + 3)2^{2j} - 1, \\
2 - 4L(\alpha), & s = (4\alpha + 1)2^{2j} - 1, \\
-1 + 2L(\alpha), & s = (4\alpha + 3)2^{2j+1} - 1, \\
3 + 2L(\alpha) + 4\alpha, & s = (4\alpha + 1)2^{2j+1} - 1.
\end{cases} \\
M(4s + 3) &\equiv_{8} \begin{cases} 
-2 + 4L(\alpha), & s = (4\alpha + 3)2^{2j} - 1, \\
4, & s = (4\alpha + 1)2^{2j} - 1, \\
-1 + 2L(\alpha), & s = (4\alpha + 3)2^{2j+1} - 1, \\
-1 + 2L(\alpha) + 4\alpha, & s = (4\alpha + 1)2^{2j+1} - 1.
\end{cases}
\end{align*}
\]

Proof. By Lemma 12, the odd case is reduced to the even case.
For \( M(4s + 1) \), we have
\[ M(4s + 1) \equiv_{8} (4s + 1)M(4s) \]
\[ \equiv_{8} 4s + M(4s). \]
\begin{align*}
\begin{cases}
1 - 2L(\alpha) + 4\alpha, & s = 2\alpha, \\
1 - 2L(\alpha) + 4, & s = 2\alpha + 1.
\end{cases}
\end{align*}

For \( M(4s + 2) \), let \( \beta \) be odd. We simplify (9') using Lemma 12 and (12).

\[ M(\beta 2^{a+2} - 2) - M(\beta 2^{a+1} - 2) \equiv_8 M((2\alpha + 1)2^{a+2} - 4) + f((2\alpha + 1)2^{a+1} - 2) \]
\[ \equiv_8 \begin{cases}
1 - 2L((\beta - 1)/2) + 2(\beta - 1) & a = 0, \\
1 - 2L(\beta 2^{a-1} - 1) & a > 0.
\end{cases} \tag{13}
\]

Lemma 10 gives \( L(2s + 1) + L(s) \equiv_4 1 \). Thus we have

\[ M(\beta 2^{a+3} - 2) - M(\beta 2^{a+1} - 2) \equiv_8 2 - 2 \left( L(\beta 2^{a-1} - 1) + L(\beta 2^a - 1) \right) \equiv_8 0, \quad a > 0. \]

This reduces \( M(\beta 2^{a+1} - 2) \) to the \( a = 0 \) and \( a = 1 \) case.

Moreover, setting \( a = 1 \) in (13) gives

\[ M(8\beta - 2) \equiv_8 M(4\beta - 2) + 1 - 2L(\beta - 1); \]

Setting \( a = 0 \) in (13) gives

\[ M(4\beta - 2) \equiv_8 M(2\beta - 2) + 1 - 2L((\beta - 1)/2) + 2(\beta - 1). \]

i) When \( \beta = 4\alpha + 1 \), we have

\[ M((4\alpha + 1)2^{2a+2} - 2) \equiv_8 M(4(4\alpha + 1) - 2) \equiv_8 M(8\alpha) + 1 - 2L(2\alpha) \]
\[ \equiv_8 1 - 2L(\alpha) + 4\alpha + 1 - 2(2\alpha + L(\alpha)) \]
\[ \equiv_8 2 - 4L(\alpha). \]

Consequently,

\[ M((4\alpha + 1)2^{2a+3} - 2) \equiv_8 M(8(4\alpha + 1) - 2) \equiv_8 2 - 4L(\alpha) + 1 - 2L(4\alpha) \]
\[ \equiv_8 3 - 4L(\alpha) - 2(4\alpha + 2\alpha + L(\alpha)) \]
\[ \equiv_8 3 + 2L(\alpha) + 4\alpha. \]

ii) When \( \beta = 4\alpha + 3 \), we obtain

\[ M((4\alpha + 3)2^{2a+2} - 2) \equiv_8 M(4(4\alpha + 3) - 2) \equiv_8 M(8\alpha + 4) + 1 - 2L(2\alpha + 1) + 4(2\alpha + 1) \]
\[ = 1 - 2L(\alpha) + 1 - 2(1 - L(\alpha)) + 4 \]
\[ = 4. \]

Consequently,

\[ M((4\alpha + 3)2^{2a+3} - 2) \equiv_8 M(8(4\alpha + 3) - 2) \equiv_8 4 + 1 - 2L(4\alpha + 2) \]
\[ \equiv_8 5 - 2(4\alpha + 2) + L(2\alpha + 1) \]
\[ \equiv_8 1 - 2(1 - L(\alpha)) \]
Finally, we compute $M(4s + 3)$. By Lemma 12, we have

$$M(4s + 3) \equiv_8 (4s + 3)M(4s + 2) + g(2s + 1)$$

$$\equiv_8 -M(4s + 2) + 4s - 2M(4s)$$

$$\equiv_8 -M(4s + 2) + 4s - 2(1 + 2s + 2L(s))$$

$$\equiv_8 -M(4s + 2) - 2 - 4L(s).$$

i) When $\beta = 4\alpha + 1$, we obtain

$$M((4\alpha + 1)2^{2a+2} - 1) \equiv_8 -M((4\alpha + 1)2^{2a+2} - 2) - 2 - 4L((4\alpha + 1)2^{2a} - 1)$$

$$\equiv_8 -2 + 4L(\alpha) - 2 - 4L(\alpha)$$

$$\equiv_8 4.$$

In the same way,

$$M((4\alpha + 1)2^{2a+3} - 1) \equiv_8 -M((4\alpha + 1)2^{2a+3} - 2) - 2 - 4L((4\alpha + 1)2^{2a+1} - 1)$$

$$\equiv_8 -3 - 2L(\alpha) - 4\alpha - 2 - 4L(\alpha) + 4$$

$$\equiv_8 -1 + 4\alpha + 2L(\alpha).$$

ii) When $\beta = 4\alpha + 3$, we have

$$M((4\alpha + 3)2^{2a+2} - 1) \equiv_8 -M((4\alpha + 3)2^{2a+2} - 2) - 2 - 4L((4\alpha + 3)2^{2a} - 1)$$

$$\equiv_8 -4 - 2 - 4L(\alpha) + 4$$

$$\equiv_8 -2 + 4L(\alpha).$$

In the same way,

$$M((4\alpha + 3)2^{2a+3} - 1) \equiv_8 -M((4\alpha + 3)2^{2a+3} - 2) - 2 - 4L((4\alpha + 3)2^{2a+1} - 1)$$

$$\equiv_8 1 - 2L(\alpha) - 2 - 4L(\alpha)$$

$$\equiv_8 -1 + 2L(\alpha).$$

\[\square\]

References


