

REPRESENTATION OF A 2-POWER AS SUM OF k 2-POWERS: A RECURSIVE FORMULA

A. GIORGILLI AND G. MOLteni

Abstract. For every integer k , a k -representation of 2^{k-1} is a string $\mathbf{n} = (n_1, \dots, n_k)$ of non-negative integers such that $\sum_{j=1}^k 2^{n_j} = 2^{k-1}$, and $\mathcal{W}(1, k)$ is their number. We present a powerful recursive formula for $\mathcal{W}(1, k)$; as a byproduct we prove the interesting congruence $\mathcal{W}(1, k) = 4 + (-1)^k \pmod{8}$ for $k \geq 3$.

2000 Mathematics Subject Classification: 11A99, 11B65

Key words: k -representations, Sierpiński's gasket, Lucas' theorem

1. INTRODUCTION AND MAIN RESULT

A k -representation of an integer ℓ is a string $\mathbf{n} = (n_1, \dots, n_k)$ of non-negative integers such that $\sum_{j=1}^k 2^{n_j} = \ell$, strings differing by the order being considered as distinct. We denote by $\mathcal{U}(\ell, k)$ the number of k -representations of ℓ :

$$\mathcal{U}(\ell, k) := \#\{\mathbf{n} = (n_1, \dots, n_k) \in \mathbb{N}^k : \sum_{j=1}^k 2^{n_j} = \ell\}.$$

It is also interesting to consider the constants $\max_{\ell} \{\mathcal{U}(\ell, k)\}$. E.g., in the paper [8] of the second author the latter constants have been used in order to prove the existence of a cancellation in exponential sums of type $\sum_{k=1}^{\tau} \zeta^{2^k}$ where ζ is q -th primitive root of unity, q is an odd integer and τ is the order of 2 modulo q , in the *short* range $\tau \asymp \log q$. Actually, as it will be seen below, the calculation of $\max_{\ell} \{\mathcal{U}(\ell, k)\}$ may be reduced to that one of the values of $\mathcal{U}(\ell, k)$ for $\ell = 2^{k-1}$.

In the present paper we obtain a recursive formula which allows us to compute the sequence $\mathcal{U}(2^{k-1}, k)$ in a very effective manner. For instance, we could calculate the latter sequence up to $k \asymp 500$ in less than 10 seconds of CPU time on a conventional PC, and we could reach $k \asymp 2000$ in a little more than one hour. Actually, the quality of the results in [8] has been greatly affected by our ability to calculate such constants. The formula will be stated in Theorem 1 below.

Let us begin with a few considerations. For every fixed k , the sequence $\mathcal{U}(\ell, k)$ as depending on ℓ exhibits a very chaotic pattern. However, a more regular behaviour shows up if one considers the related quantities $\mathcal{W}(\sigma, k) = \max_{\ell: \sigma(\ell)=\sigma} \{\mathcal{U}(\ell, k)\}$ where $\sigma(\ell)$ is the Hamming weight of ℓ , i.e. the number of digits 1 appearing in the binary representation of ℓ . Actually, the calculation of the double indexed sequence $\mathcal{W}(\sigma, k)$ for $\sigma > 1$ is an easy matter if the

sequence $\mathcal{W}(1, k)$ is known thanks to the formula (see [8] for a proof)

$$(1) \quad \mathcal{W}(\sigma, k) = k! \sum_{\substack{k_1, \dots, k_\sigma \geq 1 \\ k_1 + \dots + k_\sigma = k}} \prod_{j=1}^{\sigma} \frac{\mathcal{W}(1, k_j)}{k_j!}.$$

An equivalent way to state the latter identity is by saying that $L_\sigma(x) = (L_1(x))^\sigma$, where $L_\sigma(x)$ is the formal series $\sum_{k=1}^{+\infty} \frac{\mathcal{W}(\sigma, k)}{k!} x^k$. The recursive identity $L_\sigma(x) = L_1(x)L_{\sigma-1}(x)$ immediately gives the formula

$$\mathcal{W}(\sigma, k) = k! \sum_{n=1}^{k-1} \frac{\mathcal{W}(1, n)}{n!} \cdot \frac{\mathcal{W}(\sigma-1, k-n)}{(k-n)!}$$

which is a very quick formula to compute $\mathcal{W}(\sigma, k)$ iteratively from a given set of values for $\mathcal{W}(1, k)$.

Thus, we need a way to calculate the sequence $\mathcal{W}(1, k)$. Now, the definition of $\mathcal{W}(1, k)$ as $\max_w \{\mathcal{U}(2^w, k)\}$ is not satisfactory unless we can determine for which $w = w(k)$ the maximum is reached. Luckily this can be done simply. In fact, let \mathbf{n} be a k -representation of 2^w , then $\mathbf{n}' := \mathbf{n} + (1, \dots, 1)$ is a k -representation of 2^{w+1} . This proves that $\mathcal{U}(2^w, k) \leq \mathcal{U}(2^{w+1}, k)$ for every w , i.e. that the sequence $\mathcal{U}(2^w, k)$ increases with w . When $w \geq k-1$ the argument can be reversed, because in this case each entry in any k -representation of 2^{w+1} is strictly positive (see Lemma 1 of [8]). It follows that $\mathcal{U}(2^w, k) = \mathcal{U}(2^{w+1}, k)$ for $w \geq k-1$. We conclude that $\mathcal{W}(1, k) = \mathcal{U}(2^{k-1}, k)$. We emphasize that the naive approach, namely calculating the latter quantity by searching all k -representation of 2^{k-1} , is definitely impractical in view of the fact that the number of such representations grows as $C^k k!$ with some $C > 1$. Theorem 1 below provides an effective way to do the job. As a byproduct, we will also be able to prove in Theorem 2 a curious arithmetical property of these numbers.

Theorem 1. *Let $M_{k,l}$ be the two indexes sequence defined as*

$$(2a) \quad M_{k,l} = 0 \quad \text{if } l \geq k,$$

$$(2b) \quad M_{k,k-1} = 1 \quad \text{if } k > 1,$$

$$(2c) \quad M_{k,l} = \sum_{s=1}^{2l} \binom{k+l-1}{2l-s} M_{k-l,s} \quad \text{if } 1 \leq l < k-1.$$

Then $\mathcal{W}(1, k) = M_{k,1}$ for all $k > 1$.

2. PROOF OF THEOREM 1

The proof requires several definitions and lemmas. Let $\mathcal{R}_{k,l}$ be the set of vectors of nonnegative integers where the first entry is l , each further entry is two times the previous one at most, and whose sum is $k-1$; in other words

$$\mathcal{R}_{k,l} := \{\mathbf{r} \in \mathbb{N}^{k-1} : r_1 = l, 0 \leq r_s \leq 2r_{s-1} \forall s, r_1 + r_2 + \dots + r_{k-1} = k-1\}.$$

Moreover, let the *weight* of a vector $\mathbf{r} \in \mathcal{R}_{k,l}$ be the integer

$$\nu_{k,l}(\mathbf{r}) := \frac{(k+l-1)!}{(2r_1 - r_2)! \cdots (2r_{k-2} - r_{k-3})! (2r_{k-1})!}.$$

Lemma 1. For $k > 1$ let $M_{k,l} := \sum_{\mathbf{r} \in \mathcal{R}_{k,l}} \nu_{k,l}(\mathbf{r})$; the sequence $M_{k,l}$ satisfies the recursive laws in (2).

Proof. The definition of \mathcal{R}_{kl} shows that $\mathcal{R}_{k,l} = \emptyset$ when $l \geq k$, proving (2a); besides, $\mathcal{R}_{k,k-1}$ contains the unique vector $(k-1, 0, \dots, 0)$ whose weight is 1, hence also (2b) is proved. At last, the set $\mathcal{R}_{k,l}$ can be recursively generated, because

$$\mathcal{R}_{k,l} = \bigcup_{1 \leq s \leq 2l} \{(l, \mathbf{r}'), \mathbf{r}' \in \mathcal{R}_{k-l,s}\}.$$

This formula gives

$$\begin{aligned} M_{k,l} &= \sum_{\mathbf{r} \in \mathcal{R}_{k,l}} \nu_{k,l}(\mathbf{r}) = \sum_{s=1}^{2l} \sum_{\mathbf{r}' \in \mathcal{R}_{k-l,s}} \nu_{k,l}((l, \mathbf{r}')) \\ &= \sum_{s=1}^{2l} \sum_{\mathbf{r}' \in \mathcal{R}_{k-l,s}} \frac{(k+l-1)!}{(2l-r'_1)! \cdots (2r'_{k-3}-r'_{k-4})!(2r'_{k-2})!} \\ &= \sum_{s=1}^{2l} \frac{(k+l-1)!}{(2l-s)!(k-l+s-1)!} \sum_{\mathbf{r}' \in \mathcal{R}_{k-l,s}} \frac{(k-l+s-1)!}{(2r'_1-r'_2)! \cdots (2r'_{k-3}-r'_{k-4})!(2r'_{k-2})!} \\ &= \sum_{s=1}^{2l} \binom{k+l-1}{2l-s} \sum_{\mathbf{r}' \in \mathcal{R}_{k-l,s}} \nu_{k-l,s}(\mathbf{r}') = \sum_{s=1}^{2l} \binom{k+l-1}{2l-s} M_{k-l,s}, \end{aligned}$$

which is (2c). \square

For every $s \in \mathbb{N}$ and $\mathbf{n} = (n_1, \dots, n_m) \in \mathbb{Z}^m$ with $m \geq s$, we define $\phi_0(\mathbf{n}) := \mathbf{n}$ while for $s > 0$ we set

$$\phi_s(\mathbf{n}) := (n_1 - 1, n_1 - 1, n_2 - 1, n_2 - 1, \dots, n_s - 1, n_s - 1, n_{s+1}, \dots, n_m);$$

in other words, ϕ_s subtracts one to the first s entries of \mathbf{n} and double them in number. The following facts have an immediate proof:

- (a) $\phi_s(\mathbf{n}) \in \mathbb{Z}^{m+s}$;
- (b) if the string \mathbf{n} is not decreasing, then $\phi_s(\mathbf{n})$ is not decreasing, too;
- (c) $\sum_{j=1}^m 2^{n_j} = \sum_{j=1}^{m+s} 2^{\phi_s(\mathbf{n})_j}$.

For every $\mathbf{r} \in \mathcal{R}_{k,1}$, we define the map $\psi_{\mathbf{r}} := \phi_{r_{k-1}} \circ \phi_{r_{k-2}} \cdots \circ \phi_{r_1}$. At last, let \mathcal{N}_k be the set of ordered k -representations of 2^{k-1} , i.e.

$$\mathcal{N}_k := \{\mathbf{n} \in \mathbb{N}^k : n_1 \leq n_2 \leq \cdots \leq n_k, \sum_{j=1}^k 2^{n_j} = 2^{k-1}\}.$$

Lemma 2. When $k > 1$ the map ψ sending \mathbf{r} to $\psi_{\mathbf{r}}((k-1))$ is a bijection between $\mathcal{R}_{k,1}$ and \mathcal{N}_k .

Proof. The definition of $\psi_{\mathbf{r}}$ as $\phi_{r_{k-1}} \circ \phi_{r_{k-2}} \cdots \circ \phi_{r_1}$ and (a) show that $\psi_{\mathbf{r}}((k-1))$ is a vector in $\mathbb{Z}^{1+\sum_j r_j} = \mathbb{Z}^k$. Each map ϕ_s decreases the entries of its argument of a unity, at most, hence the map $\psi_{\mathbf{r}}$ for $\mathbf{r} \in \mathcal{R}_{k,1}$ decreases the entries of its argument of $k-1$, at most: this implies that the entries of $\psi_{\mathbf{r}}((k-1))$ are

nonnegative. Finally, by (c) we conclude that $\psi_{\mathbf{r}}((k-1))$ is a k -representation of 2^{k-1} , which is in \mathcal{N}_k by (b).

It is not difficult to convince oneself that

$$(3) \quad \psi_{\mathbf{r}}((k-1)) = \left(\underbrace{0}_{2r_{k-1} \text{ times}}, \underbrace{1}_{2r_{k-2} - r_{k-1} \text{ times}}, \dots, \underbrace{k-3}_{2r_2 - r_3 \text{ times}}, \underbrace{k-2}_{2r_1 - r_2 \text{ times}} \right),$$

an identity proving that ψ is one to one.

We prove that ψ is surjective by giving an explicit algorithm to generate $\mathbf{r} \in \mathcal{R}_{k,1}$ such that $\psi_{\mathbf{r}}((k-1)) = \mathbf{n}$, for every $\mathbf{n} \in \mathcal{N}_k$. Let $\mathbf{n} \in \mathcal{N}_k$ be given, thus $\mathbf{n} \in \mathbb{N}^k$ with $\sum_{j=1}^k 2^{n_j} = 2^{k-1}$ and $n_1 \leq n_2 \leq \dots \leq n_k$. If n_1 is not 0, we take $r_{k-1} = r_{k-2} = \dots = r_{k-n_1} = 0$; this is the unique choice for these components of \mathbf{r} which accords with (3). Let m be the index such that $n_1 = n_2 = \dots = n_m < n_{m+1}$, where the last inequality is meaningful only if $m < k$. Under the assumption $k > 1$ the number n_1 is strictly lower than $k-1$, therefore the equality $\sum_{j=1}^k 2^{n_j} = 2^{k-1}$ considered modulo 2^{n_1+1} produces the congruence $m2^{n_1} = 0 \pmod{2^{n_1+1}}$, proving that m is even. We set $r_{k-n_1-1} = m/2$ and substitute \mathbf{n} with a new and shorter vector

$$\mathbf{n}' := \left(\underbrace{n_1 + 1}_{m/2 \text{ times}}, n_{m+1}, \dots, n_k \right).$$

The previous arguments prove that $\mathbf{n} = (\phi_{r_{k-1}} \circ \dots \circ \phi_{r_{k-n_1}} \circ \phi_{r_{k-n_1-1}})(\mathbf{n}')$. A congruence modulo 2^{n_1+2} shows that the number m' of entries in \mathbf{n}' with value $n_1 + 1$ is even, therefore we can set $r_{k-n_1-2} = m'/2$, obtaining that $\mathbf{n}' = \phi_{r_{k-n_1-2}}(\mathbf{n}'')$ for a suitable \mathbf{n}'' . This process can be repeated $k - n_1$ times and produces the required vector \mathbf{r} in $\mathcal{R}_{k,1}$. \square

Now we can conclude the proof of Theorem 1. We say that two k -representations of 2^{k-1} \mathbf{n} and \mathbf{n}' are equivalent when there exists a permutation π such that $\pi(\mathbf{n}) = \mathbf{n}'$. This relation is evidently an equivalence and \mathcal{N}_k is a set of representatives. Denoting by $\mu(\mathbf{n})$ the number of k -representations of 2^{k-1} which are equivalent to \mathbf{n} , we have therefore that $\mathcal{W}(1, k) = \sum_{\mathbf{n} \in \mathcal{N}_k} \mu(\mathbf{n})$. By Lemma 2 we know that $\mathbf{n} = \psi(\mathbf{r})$ for some $\mathbf{r} \in \mathcal{R}_{k,1}$ and by (3) we see that $\mu(\mathbf{n}) = \nu_{k,1}(\mathbf{r})$, therefore we conclude that $\mathcal{W}(1, k) = \sum_{\mathbf{r} \in \mathcal{R}_{k,1}} \nu_{k,1}(\mathbf{r})$ which is $M_{k,1}$, by definition.

3. A CONGRUENCE

Let \mathcal{T} be the infinite matrix defined as the limit of the matrices T_n with

$$T_0 = (1), \quad T_{n+1} = \begin{pmatrix} T_n & 0 \\ T_n & T_n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \otimes T_n \quad \text{for } n > 0,$$

where the limit is taken with respect to the evident inclusion $T_n \subset T_{n+1}$. The matrix \mathcal{T} is the prototype of a discrete self-similar set and is strictly connected to the ‘‘Sierpiński’s gasket’’. In a seminal paper, Lucas [7] proved a very efficient way to compute the residue of the binomial coefficients modulo any fixed prime p (for an elegant alternative proof of his result see also [3]).

When $p = 2$ his result says that

$$(4) \quad \binom{2a + a_0}{2b + b_0} = \binom{a}{b} \binom{a_0}{b_0} \pmod{2},$$

for every $a, b \in \mathbb{N}$, for every $a_0, b_0 \in \{0, 1\}$. An equivalent statement says that $\binom{a}{b}$ is odd iff a dominates b , in symbols $a \succeq b$, where ‘ a dominates b ’ means that if $a = \sum_j a_j 2^j$ and $b = \sum_j b_j 2^j$ are the binary representations of a and b , then $a_j \geq b_j$ for every j . This result proves that if we take the residues of the entire Pascal’s triangle modulo 2 we get exactly the self-similar set \mathcal{T} (see also [4]).

The interest of this result for the present paper comes from the fact that, quite surprisingly, the set \mathcal{T} appears also when our matrix $M_{k,l}$ is reduced modulo 2. In view of the different normalization of the indexes this remark can be stated by saying that $M_{k,l} = \binom{k-2}{l-1} \pmod{2}$ for every k, l with $k \geq 2$.

Recently also the residues of the binomial coefficients modulo prime powers have been enquired by many authors [1, 2, 5, 6]. The following congruences are simple consequences of the result in [1]:

$$(5) \quad \binom{2a + 1}{2b + 1} = (-1)^{a(b+1)} \binom{a}{b} \pmod{4}, \quad \binom{2a}{2b} = \binom{a}{b} \pmod{4}.$$

The analogy between our matrix $M_{k,l}$ and the binomial coefficients is preserved also at higher powers of 2: in fact, in this section we prove the following result

Theorem 2. For $k \geq 3$,

$$M_{k,l} = (-1)^{kl} \binom{k-2}{l-1} + 4(\mathcal{T} \otimes A)_{k-2,l} \pmod{8}, \quad \text{where } A := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

An immediate consequence of this result is that $\mathcal{W}(1, k) = M_{k,1} = 4 + (-1)^k \pmod{8}$ for $k \geq 3$, a fact that we were unable to prove in a more direct way.

The pattern shown by $M_{k,l}$ modulo 2^m with $m > 3$ is very complicated, much more complicated than that one of the binomial coefficients; nevertheless a some kind of regularity is still preserved; for example, the values of $\mathcal{W}(1, k) = M_{k,1}$ modulo 2^m seem to be definitively periodic even for $m > 3$. At present we are unable to prove this fact.

Our numerical calculations show that any regularity disappears when the residues of $M_{k,l}$ are considered modulo powers of odd primes: the analogy between $M_{k,l}$ and the binomial is therefore limited to the powers of 2.

For the proof of Theorem 2 we need some preliminary lemmas.

Lemma 3. Let $\mathcal{F}_{k,l} := \sum_{s=1}^{2l} \binom{k+l-1}{2l-s} (-1)^{(k-l)s} \binom{k-l-2}{s-1}$; the following equality holds modulo 8:

$$\mathcal{F}_{k,l} = \begin{cases} \binom{2(k-2)+1}{2(l-1)+1} & \text{if } k-l = 0 \pmod{2} \\ -\binom{2(k-2)+1}{2(l-1)+1} + 2\binom{k-2}{l-1} & \text{if } k-l = 3 \pmod{4} \\ -\binom{2(k-2)+1}{2(l-1)+1} - 2\binom{k-2}{l-1} + 4\binom{\lfloor \frac{k-3}{2} \rfloor}{\lfloor \frac{l-2}{2} \rfloor} & \text{if } k-l = 1 \pmod{4}. \end{cases}$$

Proof. The proof is an elementary calculation using the Vandermonde identity $\sum_{j=0}^w \binom{m}{w-j} \binom{n}{j} = \binom{m+n}{w}$ and Congruences (4)-(5). In fact, suppose $k - l = 0 \pmod{2}$, then $\mathcal{F}_{k,l} = \sum_{s=0}^{2l-1} \binom{k+l-1}{2l-1-s} \binom{k-l-2}{s}$ that by Vandermonde equals $\binom{2k-3}{2l-1}$. Suppose now $k - l = 1 \pmod{2}$, then

$$\begin{aligned} \mathcal{F}_{k,l} &= - \sum_{s=0}^{2l-1} (-1)^s \binom{k+l-1}{2l-1-s} \binom{k-l-2}{s} \\ &= - \sum_{s=0}^{2l-1} \binom{k+l-1}{2l-1-s} \binom{k-l-2}{s} + 2 \sum_{\substack{s=0 \\ s \text{ odd}}}^{2l-1} \binom{k+l-1}{2l-1-s} \binom{k-l-2}{s} \end{aligned}$$

that by Vandermonde becomes

$$= - \binom{2k-3}{2l-1} + 2 \sum_{u=0}^{l-1} \binom{2\frac{k+l-1}{2}}{2(l-1-u)} \binom{2\frac{k-l-3}{2} + 1}{2u+1}.$$

Recalling that we are computing modulo 8 and using the congruences in (5) we conclude that

$$(6) \quad \mathcal{F}_{k,l} = - \binom{2k-3}{2l-1} + 2 \sum_{u=0}^{l-1} \binom{\frac{k+l-1}{2}}{l-1-u} (-1)^{\frac{k-l-3}{2}(u+1)} \binom{\frac{k-l-3}{2}}{u}.$$

Suppose $k - l = 3 \pmod{4}$, then we have

$$\mathcal{F}_{k,l} = - \binom{2k-3}{2l-1} + 2 \sum_{u=0}^{l-1} \binom{\frac{k+l-1}{2}}{l-1-u} \binom{\frac{k-l-3}{2}}{u} = - \binom{2k-3}{2l-1} + 2 \binom{k-2}{l-1}$$

by Vandermonde, again. On the contrary, suppose $k - l = 1 \pmod{4}$, then (6) gives

$$\begin{aligned} \mathcal{F}_{k,l} &= - \binom{2k-3}{2l-1} - 2 \sum_{u=0}^{l-1} \binom{\frac{k+l-1}{2}}{l-1-u} (-1)^u \binom{\frac{k-l-3}{2}}{u} \\ &= - \binom{2k-3}{2l-1} - 2 \sum_{u=0}^{l-1} \binom{\frac{k+l-1}{2}}{l-1-u} \binom{\frac{k-l-3}{2}}{u} + 4 \sum_{\substack{u=0 \\ u \text{ odd}}}^{l-1} \binom{\frac{k+l-1}{2}}{l-1-u} \binom{\frac{k-l-3}{2}}{u}, \end{aligned}$$

i.e.

$$(7) \quad \mathcal{F}_{k,l} = - \binom{2k-3}{2l-1} - 2 \binom{k-2}{l-1} + 4 \sum_{v=0}^{\lfloor \frac{l-2}{2} \rfloor} \binom{\frac{k+l-1}{2}}{l-2-2v} \binom{\frac{k-l-3}{2}}{2v+1}.$$

Suppose $l = 2l'$, then $k = 2k' + 1$ with $k' - l' = 0 \pmod{2}$ (because we are assuming $k - l = 1 \pmod{4}$) and from (7) we have

$$\begin{aligned} \mathcal{F}_{k,l} &= - \binom{2k-3}{2l-1} - 2 \sum_{u=0}^{l-1} \binom{k-2}{l-1} + 4 \sum_{v=0}^{l'-1} \binom{k'+l'}{2(l'-1-v)} \binom{k'-l'-1}{2v+1} \\ &= - \binom{2k-3}{2l-1} - 2 \binom{k-2}{l-1} + 4 \sum_{v=0}^{l'-1} \binom{2\frac{k'+l'}{2}}{2(l'-1-v)} \binom{2\frac{k'-l'-2}{2} + 1}{2v+1}. \end{aligned}$$

Since we are computing modulo 8, using the congruences in (4) we have

$$\mathcal{F}_{k,l} = -\binom{2k-3}{2l-1} - 2\binom{k-2}{l-1} + 4\sum_{v=0}^{l'-1} \binom{\frac{k'+l'}{2}}{l'-1-v} \binom{\frac{k'-l'-2}{2}}{v}$$

that by Vandermonde gives

$$\mathcal{F}_{k,l} = -\binom{2k-3}{2l-1} - 2\binom{k-2}{l-1} + 4\binom{k'-1}{l'-1}$$

which agrees with the claim, since $\lfloor \frac{k-3}{2} \rfloor = k' - 1$ and $\lfloor \frac{l-2}{2} \rfloor = l' - 1$. Finally, suppose $l = 2l' + 1$, then $k = 2k'$ with $k' - l' = 1 \pmod{2}$ and from (7) we have

$$\begin{aligned} \mathcal{F}_{k,l} &= -\binom{2k-3}{2l-1} - 2\sum_{u=0}^{l-1} \binom{k-2}{l-1} + 4\sum_{v=0}^{l'-1} \binom{k'+l'}{2l'-1-2v} \binom{k'-l'-2}{2v+1} \\ &= -\binom{2k-3}{2l-1} - 2\binom{k-2}{l-1} + 4\sum_{v=0}^{l'-1} \binom{2\frac{k'+l'-1}{2}+1}{2(l'-1-v)+1} \binom{2\frac{k'-l'-3}{2}+1}{2v+1}. \end{aligned}$$

As before, using the congruences in (4) we have

$$= -\binom{2k-3}{2l-1} - 2\binom{k-2}{l-1} + 4\sum_{v=0}^{l'-1} \binom{\frac{k'+l'-1}{2}}{l'-1-v} \binom{\frac{k'-l'-3}{2}}{v}$$

that by Vandermonde gives

$$= -\binom{2k-3}{2l-1} - 2\binom{k-2}{l-1} + 4\binom{k'-2}{l'-1}$$

which agrees with the claim, since $\lfloor \frac{k-3}{2} \rfloor = k' - 2$ and $\lfloor \frac{l-2}{2} \rfloor = l' - 1$. \square

Lemma 4. For $k \geq 3$ and $l \geq 1$ we have modulo 8:

$$\mathcal{F}_{k,l} - (-1)^{kl} \binom{k-2}{l-1} = 4(\mathcal{T} \otimes B)_{k-2,l} \quad \text{where } B := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Proof. By Lemma 3 we must prove that

$$\begin{aligned} (-1)^{k-l} \binom{2k+1}{2(l-1)+1} + 2\delta_{k-l=1(2)} (-1)^{\frac{k-l-1}{2}} \binom{k}{l-1} + 4\delta_{k-l=3(4)} \binom{\lfloor \frac{k-1}{2} \rfloor}{\lfloor \frac{l-2}{2} \rfloor} \\ - (-1)^{kl} \binom{k}{l-1} = 4(\mathcal{T} \otimes B)_{k,l} \pmod{8} \quad \forall k \geq 1. \end{aligned}$$

In this equality the indexes k, l are ≥ 1 ; since the entries $(\mathcal{T} \otimes B)_{k,l}$ depend on the binary representation of $k-1$ and $l-1$, *only in this proof* it is convenient to shift the indexes by setting $k \leftarrow k-1$, $l \leftarrow l-1$. After this shift the claim

becomes

$$\begin{aligned} & (-1)^{k-l} \binom{2(k+1)+1}{2l+1} + 2\delta_{k-l=1(2)} (-1)^{\frac{k-l-1}{2}} \binom{k+1}{l} + 4\delta_{k-l=3(4)} \binom{\lfloor \frac{k}{2} \rfloor}{\lfloor \frac{l-1}{2} \rfloor} \\ & - (-1)^{(k+1)(l+1)} \binom{k+1}{l} = 4(\mathcal{T} \otimes B)_{k,l} \pmod{8} \quad \forall k, l \geq 0, \end{aligned}$$

where now in $\mathcal{T} \otimes B$ the indexes start by 0. The claim is evident for $l \geq k+1$ because both LHS and RHS are zero; in particular both LHS and RHS are triangular matrices and we can assume $l \leq k$. The proof splits in four cases, according to the parities of k and l .

- $k = 2k'$ and $l = 2l' + 1$. Since $(\mathcal{T} \otimes B)_{2k', 2l'+1} = 0$, the congruence modulo 8 becomes

$$(8) \quad -\binom{4k'+3}{4l'+3} - (2(-1)^{k'-l'} + 1) \binom{2k'+1}{2l'+1} + 4\delta_{k'-l'=0(2)} \binom{k'}{l'} = 0.$$

- Suppose $k = 2k'$ and $l = 2l'$. Since $(\mathcal{T} \otimes B)_{2k', 2l'} = (\mathcal{T} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix})_{k', l'}$, the congruence modulo 8 becomes

$$(9) \quad \binom{4k'+3}{4l'+1} + \binom{2k'+1}{2l'} = 4\delta_{\substack{k', l' \text{ even} \\ l'/2 \leq k'/2}}.$$

- Suppose $k = 2k' + 1$ and $l = 2l' + 1$. Since $(\mathcal{T} \otimes B)_{2k'+1, 2l'+1} = 0$, the congruence modulo 8 becomes

$$(10) \quad -\binom{4k'+5}{4l'+3} - \binom{2k'+2}{2l'+1} = 0.$$

- Suppose $k = 2k' + 1$ and $l = 2l'$. Since $(\mathcal{T} \otimes B)_{2k'+1, 2l'} = (\mathcal{T} \otimes \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix})_{k', l'}$, the congruence modulo 8 becomes

$$(11) \quad -\binom{4k'+5}{4l'+1} + (2(-1)^{k'-l'} - 1) \binom{2k'+2}{2l'} + 4\delta_{k'-l'=1(2)} \binom{k'}{l'-1} = 4\delta_{\substack{l' \text{ even} \\ l'/2 \leq \lfloor k'/2 \rfloor}}.$$

Congruences (8)–(11) can be proved using the result in [1], since it allows to write $\binom{2a+a_0}{2b+b_0}$ as $C_{a,b,a_0,b_0} \binom{a}{b}$ modulo 8 where C_{a,b,a_0,b_0} is explicitly given and depends only on a_0, b_0 and the residues modulo 4 of a and b . For example, using this result we can reduce (8) to a congruence where to LHS we have $C'_{k',l'} \binom{k'}{l'}$ with an explicit $C'_{k',l'}$ depending only on residues modulo 4 of k' and l' . A new application of [1] allows us to prove that in any case LHS is divisible by 8. A similar approach can be used for (9) and (10). For (11) we also use the relation $\binom{k'+1}{l'} = \frac{k'+1}{l'} \binom{k'}{l'-1}$. We leave to the reader the (very tedious) task to verify all the details of this proof. \square

Now we study the behaviour of

$$\mathcal{G}_{k,l} := \sum_{s=1}^{2l} \binom{k+l-1}{2l-s} (\mathcal{T} \otimes A)_{k-l-2,s} \pmod{2}, \quad k \geq 4, 1 \leq l \leq k-3.$$

Lemma 5. For $k \geq 4$ we have

$$\mathcal{G}_{k,l} = (\mathcal{T} \otimes C)_{k-2,l}, \quad \text{where } C := \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Proof. In other words, we have to prove that for $k \geq 1$, $\mathcal{G}_{k+2,l} = (\mathcal{T} \otimes C)_{k,l}$ where

$$\mathcal{G}_{k+2,l} = \sum_{s=1}^{2l} \binom{k+l+1}{2l-s} (\mathcal{T} \otimes A)_{k-l,s} \pmod{2}.$$

We prove this equality by considering separately the different classes of $k-l$ modulo 4.

- Suppose $k-l$ odd. Then $(\mathcal{T} \otimes A)_{k-l,s} = 1$ only for odd values of s ; assuming s odd we have

$$\binom{k+l+1}{2l-s} = \binom{2^{\frac{k+l+1}{2}}}{2(l - \frac{s+1}{2}) + 1} \pmod{2} = 0$$

where (4) has been used for the last equality. It follows that under this assumption $\mathcal{G}_{k+2,l} = 0$, which is also the value of $(\mathcal{T} \otimes C)_{k,l}$ under this hypothesis.

- Suppose $k-l = 0 \pmod{4}$. Then the set of integers s where $(\mathcal{T} \otimes A)_{k-l,s} = 1$ is made of couples $a, a+1$, for suitable odd integers a . We have

$$\begin{aligned} \binom{k+l+1}{2l-a} + \binom{k+l+1}{2l-a-1} &= \binom{2^{\frac{k+l}{2}} + 1}{2(l - \frac{a+1}{2}) + 1} + \binom{2^{\frac{k+l}{2}} + 1}{2(l - \frac{a+1}{2})} \\ &= \binom{\frac{k+l}{2}}{l - \frac{a+1}{2}} + \binom{\frac{k+l}{2}}{l - \frac{a+1}{2}} = 0 \pmod{2} \end{aligned}$$

where (4) has been used for the second equality. It follows that also in this case $\mathcal{G}_{k+2,l} = 0$. It is easy to verify that also $(\mathcal{T} \otimes C)_{k,l}$ is null under the assumption $k = l \pmod{4}$, hence the congruence is proved in this case, as well.

- Suppose $k-l = 2 \pmod{4}$. Then the set of integers s where $(\mathcal{T} \otimes A)_{k-l,s} = 1$ is the set $\{s : s-1 \preceq k-l-2\}$. We set $k-l-2 =: 4u$ and $l-1 =: m$. The condition $s-1 \preceq 4u$ implies that $s-1$ is a multiple of 4, $s-1 =: 4v$ say, with $v \preceq u$. In terms of u, v and m we have

$$\mathcal{G}_{k+2,l} = \sum_{\substack{v=0 \\ v \preceq u}}^{\lfloor m/2 \rfloor} \binom{4u+2m+5}{2m+1-4v} = \sum_{\substack{v=0 \\ v \preceq u}}^{\lfloor m/2 \rfloor} \binom{u + \lfloor m/2 \rfloor + 1}{\lfloor m/2 \rfloor - v} \pmod{2},$$

where for the last equality the congruence in (4) has been applied twice. The restriction $v \preceq u$ can be included in the sum by multiplying the terms by $\binom{u}{v}$. In this way we have

$$\mathcal{G}_{k+2,l} = \sum_{v=0}^{\lfloor m/2 \rfloor} \binom{u + \lfloor m/2 \rfloor + 1}{\lfloor m/2 \rfloor - v} \binom{u}{v} = \binom{2u + \lfloor m/2 \rfloor + 1}{\lfloor m/2 \rfloor} \pmod{2},$$

where for the last equality we used the Vandermonde identity. The equality we have to verify is therefore

$$\binom{2u + \lfloor m/2 \rfloor + 1}{\lfloor m/2 \rfloor} = (\mathcal{T} \otimes C)_{4u+m+3, m+1} \pmod{2}.$$

In this equality both sides assume the same value for $m = 2m'$ and $m = 2m' + 1$, hence we can confine ourself to verify it only for even m . We do it by distinguishing two subcases:

- $m = 4m'$. Then $\binom{2u + \lfloor m/2 \rfloor + 1}{\lfloor m/2 \rfloor} = \binom{2u+2m'+1}{2m'} = \binom{u+m'}{m'} \pmod{2}$, and

$$(\mathcal{T} \otimes C)_{4u+m+3, m+1} = (\mathcal{T} \otimes C)_{4(u+m')+3, 4m'+1} = \begin{cases} (\mathcal{T} \otimes C)_{3,1} & \text{if } m' \preceq u + m', \\ 0 & \text{otherwise.} \end{cases}$$

Since $(\mathcal{T} \otimes C)_{3,1} = 1$, we see that $(\mathcal{T} \otimes C)_{4u+m+3, m+1} = \delta_{m' \preceq u+m'}$ that is also the value of residue of $\binom{u+m'}{m'}$ modulo 2, thus the claim is proved.

- $m = 4m' + 2$. Then $\binom{2u + \lfloor m/2 \rfloor + 1}{\lfloor m/2 \rfloor} = \binom{2u+2m'+2}{2m'+1} = 0 \pmod{2}$, and

$$(\mathcal{T} \otimes C)_{4u+m+3, m+1} = (\mathcal{T} \otimes C)_{4(u+m'+1)+1, 4m'+3} = \begin{cases} (\mathcal{T} \otimes C)_{1,3} & \text{if } m' \preceq u + m' + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Since $(\mathcal{T} \otimes C)_{1,3} = 0$, the claim is proved in this case as well. \square

Now we can complete the proof of Theorem 2.

Proof. Let $k \geq 3$. We prove directly the cases $l \geq k - 2$. The claim holds for $l \geq k$ since under this assumption $M_{k,l} = 0$, $\binom{k-2}{l-1} = 0$ and $(\mathcal{T} \otimes A)_{k-2,l} = 0$. The claim holds for $l = k - 1$ since $M_{k,k-1} = 1$, $(-1)^{k(k-1)} \binom{k-2}{(k-1)-1} = 1$ and $(\mathcal{T} \otimes A)_{k-2,k-1} = 0$. Finally, the claim holds for $l = k - 2$ since

$$M_{k,k-2} = \sum_{s=1}^{2k-4} \binom{2k-3}{2k-4-s} M_{2,s} = \binom{2k-3}{2k-5} M_{2,1} = (2k-3)(k-2);$$

besides, $(-1)^{k(k-2)} \binom{k-2}{(k-2)-1} = (-1)^k(k-2)$ and $(\mathcal{T} \otimes A)_{k-2,k-2} = \delta_{k=3(4)}$, thus the congruence becomes $(2k-3)(k-2) = (-1)^k(k-2) + 4\delta_{k=3(4)} \pmod{8}$, which is true.

Suppose $k \geq 4$ and $l \leq k - 3$. Then the recursive identity in (2c) gives $M_{k,l} = \mathcal{F}_{k,l} + \mathcal{G}_{k,l}$ so that the congruence we must prove becomes

$$\mathcal{F}_{k,l} + \mathcal{G}_{k,l} = (-1)^{kl} \binom{k-2}{l-1} + 4(\mathcal{T} \otimes A)_{k-2,l} \pmod{8},$$

which holds by Lemmas 4–5, because $B + C = A$. \square

REFERENCES

- [1] K. S. Davis and W. A. Webb, *Lucas' theorem for prime powers*, European J. Combin. **11** (1990), no. 3, 229–233.
- [2] ———, *Pascal's triangle modulo 4*, Fibonacci Quart. **29** (1991), no. 1, 79–83.
- [3] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54** (1947), 589–592.

- [4] A. S. Fraenkel and A. Kontorovich, *The Sierpiński sieve of Nim-varieties and binomial coefficients*, Combinatorial number theory, de Gruyter, Berlin, 2007, pp. 209–227.
- [5] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253–276.
- [6] G. S. Kazandzidis, *Congruences on the binomial coefficients*, Bull. Soc. Math. Grèce (N.S.) **9** (1968), no. 1, 1–12.
- [7] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1878), 49–54.
- [8] G. Molteni, *Cancellation in a short exponential sum*, preprint.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI MILANO, VIA SALDINI 50, I-20133
MILANO, ITALY, AND ISTITUTO LOMBARDO ACCADEMIA DI SCIENZE E LETTERE
E-mail address: `antonio.giorgilli@unimi.it`

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI MILANO, VIA SALDINI 50, I-20133
MILANO, ITALY
E-mail address: `giuseppe.molteni1@unimi.it`