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 $\boldsymbol{n} = (n_1, \dots, n_k)$ of nonnegative integers such that $\sum_{j=1}^{k} 2^{n_j} = 2^{k-1}$, and $\mathcal{W}(1,k)$ is their number. We present an efficient recursive formula for $\mathcal{W}(1,k)$; this formula allows also to prove the congruence $\mathcal{W}(1,k) = 4+(-1)^k \pmod 8$ for $k \geq 3$.

J. Number Theory **133**(4), 1251–1261 (2013).

1. Introduction and main result

A k-representation of an integer ℓ is a string $\boldsymbol{n} = (n_1, \dots, n_k)$ of nonnegative 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, thus

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

For any fixed k the sequence $\mathcal{U}(\ell,k)$ admits a maximum when ℓ varies, and the second author met these constants as a part of his study of the cancellation in certain short exponential sums [9]: the result there proved depended also on the ability to compute $\max_\ell\{\mathcal{U}(\ell,k)\}$ for large k. This task cannot be done simply enumerating all the k-representations of a suitable ℓ, since this number grows more than exponentially and the computation becomes unfeasible already for small values of k. Our strategy for its computation is the following. The chaotic behavior of $\mathcal{U}(\ell,k)$ as depending on ℓ disappears if it is restricted to integers having the same number of non-zero digits in their binary representation. This suggests to introduce the new quantities $\mathcal{W}(\sigma,k) = \max_{\ell\colon \sigma(\ell)=\sigma}\{\mathcal{U}(\ell,k)\}$, where $\sigma(\ell)$ counts the number of digits 1 appearing in the binary representation of ℓ. The calculation of $\mathcal{W}(\sigma,k)$ for $\sigma > 1$ is an easy matter if the sequence $\mathcal{W}(1,k)$ is known, thanks to the recursive formula (see [9] for a proof)

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

Thus we have reduced the problem of the computation of $\max_\ell\{\mathcal{U}(\ell,k)\}$ to that of the computation of $\max_\sigma\{\mathcal{W}(\sigma,k)\}$ and then to that of $\mathcal{W}(1,k)$. The definition of $\mathcal{W}(1,k)$ as $\max_w\{\mathcal{U}(2^w,k)\}$ is not satisfactory for its computation, unless we can determine for which $w = w(k)$ the maximum is reached. Luckily this can be done, and the maximum is attained for every $w \geq k-1$, thus proving that $\mathcal{W}(1,k)$ is equal to $\mathcal{U}(2^{k-1},k)$ (see [9, Lemma 1]). Also $\mathcal{W}(1,k)$ grows more than exponentially (see [10]), and, once again, it is substantially impossible to compute these constants

2010 *Mathematics Subject Classification.* Primary 11 A 99, Secondary 11 B 65.
Key words and phrases. k-representations, Sierpiński's triangle, Lucas' theorem.

simply by searching all the k-representations of 2^{k-1}. Theorem 1 below provides an effective algorithm to do the job.

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

$$M_{k,l} = 0 \qquad \text{if } l \geq k, \tag{1a}$$

$$M_{k,k-1} = 1 \qquad \text{if } k > 1, \tag{1b}$$

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

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

This algorithm is independent of, but shows several similarities with an analogous algorithm proposed by Even and Lempel [3] to enumerate all prefix codes (also called Huffman codes) on an alphabet of two symbols. The connection comes from the characteristic-sum equation

$$\sum_{j=1}^{k} 2^{-w_j} = 1,$$

where $(w_1, \dots, w_k)$ is the word-length vector of such a code: as we see, multiplying the equation by 2^w with $w := \sum_{j=1}^{k} w_j$, we get exactly a k-representation of 2^w. Nevertheless, codes having the same word-lengths are isomorphic, thus the Even-Lempel algorithm does not compute $\mathcal{W}(1,k)$ but only the number of nonnegative solutions of $\sum_{j=1}^{k} 2^{n_j} = 2^{k-1}$ satisfying the further restriction $n_1 \leq n_2 \leq \cdots \leq n_k$.

As we have already recalled, our first application of the algorithm in Theorem 1 was essentially numerical, since it allows to compute $\mathcal{W}(1,k)$ for $k \leq 2000$ in a little more than one hour on a conventional 2008 PC. Nevertheless, recently the second author [10] has used this result also to prove that $(\mathcal{W}(1,k)/k!)^{1/k}$ tends to a constant whose value is approximatively $1.192\dots$, a fact disproving an old conjecture of Knuth privately communicated to Tarjan in early '70. Moreover, a regular pattern emerges already from the first few $\mathcal{W}(1,k)$, when they are computed modulo some fixed integer; for example all of them are odd integers! Section 3 of this paper is devoted to the proof of a second theorem generalizing this remark to congruences modulo 8, once again as a consequence of the formula in Theorem 1. Other congruences are proposed in Section 3, but that one modulo 8 is the unique which we are able to prove.

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

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

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

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

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

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

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

This formula gives

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

which is (1c). □

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

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

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

(a) $\phi_s(\boldsymbol{n})\in\mathbb{Z}^{m+s}$;
(b) if the string $\boldsymbol{n}$ is non-decreasing, then $\phi_s(\boldsymbol{n})$ is non-decreasing, too;
(c) $\sum_{j=1}^{m} 2^{n_j} = \sum_{j=1}^{m+s} 2^{\phi_s(\boldsymbol{n})_j}$.

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

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

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

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

k-representation of 2^{k-1}, which is in $\mathcal{N}_k$ by (b).
It is not difficult to get convinced that

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

an identity proving that ψ is one to one.
We prove that ψ is surjective by giving an explicit algorithm to generate $\boldsymbol{r} \in \mathcal{R}_{k,1}$ such that $\psi_{\boldsymbol{r}}((k-1)) = \boldsymbol{n}$, for every $\boldsymbol{n} \in \mathcal{N}_k$. Let $\boldsymbol{n} \in \mathcal{N}_k$ be given, thus $\boldsymbol{n} \in \mathbb{N}^k$ 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 $r_{k-1} = r_{k-2} = \ldots = r_{k-n_1} = 0$; this is the unique choice for these components of $\boldsymbol{r}$ which accords with (2). 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 less 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 $\boldsymbol{n}$ with a new and shorter vector

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

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

Now we can conclude the proof of Theorem 1. We say that two k-representations $\boldsymbol{n}$ and $\boldsymbol{n}'$ of 2^{k-1} are equivalent when there exists a permutation π such that $\pi(\boldsymbol{n}) = \boldsymbol{n}'$. This relation is evidently an equivalence and $\mathcal{N}_k$ is a set of representatives. Denoting by $\mu(\boldsymbol{n})$ the number of k-representations of 2^{k-1} which are equivalent to $\boldsymbol{n}$, we have therefore that $\mathcal{W}(1,k) = \sum_{\boldsymbol{n}\in\mathcal{N}_k} \mu(\boldsymbol{n})$. By Lemma 2 we know that $\boldsymbol{n} = \psi(\boldsymbol{r})$ for some $\boldsymbol{r} \in \mathcal{R}_{k,1}$ and by (2) we see that $\mu(\boldsymbol{n}) = \nu_{k,1}(\boldsymbol{r})$, therefore we conclude that $\mathcal{W}(1,k) = \sum_{\boldsymbol{r}\in\mathcal{R}_{k,1}} \nu_{k,1}(\boldsymbol{r})$ 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 inclusion $T_{n+1} = \left(\begin{smallmatrix} T_n & 0 \\ * & * \end{smallmatrix}\right)$. The matrix $\mathcal{T}$ is the prototype of a discrete self-similar set and is strictly connected to the Sierpiński's triangle. In a seminal paper, Lucas [8] proved a very efficient way to compute the residue of the binomial coefficients modulo any fixed prime p (for an alternative proof see [4]). When $p = 2$ his result says that

$$\binom{2a+a_0}{2b+b_0} = \binom{a}{b}\binom{a_0}{b_0} \pmod 2, \tag{3}$$

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 if and only if 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 set $\mathcal{T}$ (see also [5]).

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 studied, see for example [1, 2, 6, 7]. The following congruences are simple consequences of the result in [1]:

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

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

$$\mathcal{W}(1,k) = M_{k,1} = 4 + (-1)^k \pmod 8 \qquad \forall k \geq 3. \tag{5}$$

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; however, a some kind of regularity is still preserved. For example, we have observed (but not proved) the following congruences

$$\mathcal{W}(1,k) = (-1)^k + 4 + 8 \pmod{2^4} \qquad \forall k \geq 4,$$
$$\mathcal{W}(1,k) = (-1)^k + 4 + 8(-1)^{\lceil k/2 \rceil} + 16 \pmod{2^5} \qquad \forall k \geq 5,$$

and that, more generally, the values of $\mathcal{W}(1,k)$ modulo 2^m seem to be 2^m periodic for $k \geq m$ for every m. 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 coefficients is therefore limited to the powers of 2, but some regularity is preserved for $\mathcal{W}(1,k)$. For example, we have observed (without proof, again) that

$$\mathcal{W}(1, 8km) = (-(-1)^{(m-1)/2} + 2 + 4D)m \pmod{8m} \qquad \forall k,\ \forall m \text{ odd},$$

where $D = D(m)$ is 0 if $m = 5, 7 \pmod 8$ and 1 when $m = 1, 3 \pmod 8$. Also this conjecture can be easily generalized modulo $2^r m$ with higher powers r. At present we are unable to prove all these facts, but the congruence in Theorem 2.

Each $\mathcal{W}(1,k)$ is an odd number. This an immediate consequence of (5), but there is a simple combinatoric argument proving it; the proof runs as follows. Every k-representation $(n_1, \ldots, n_k)$ of 2^{k-1} generates a second k-representation $(n_k, \ldots, n_1)$, thus $\mathcal{W}(1,k)$ is odd if and only if the number of k-representations fixed by this transformation is odd. Each symmetric k-representation $(n_1, \ldots, n_{\lceil k/2 \rceil}, n_{\lceil k/2 \rceil + 1}, \ldots, n_k)$ produces a $\lceil k/2 \rceil$-representation of 2^{k-2} selecting the first few

$\lceil k/2\rceil$ entries (for an odd index k the last entry $n_{\lceil k/2\rceil}$ is strictly positive and must be diminished by one in order to build the representation of 2^{k-2}). This correspondence is a bijection with the $\lceil k/2\rceil$-representations of 2^{k-2}. Since $2^{k-2}\geq 2^{\lceil k/2\rceil-1}$ for $k\geq 2$, the number of $\lceil k/2\rceil$-representations of 2^{k-2} is $\mathcal{W}(1,\lceil k/2\rceil)$, thus the argument proves that

$$\mathcal{W}(1,k)=\mathcal{W}(1,\lceil k/2\rceil)\pmod 2\qquad\forall k\geq 2,$$

and we can deduce that each $\mathcal{W}(1,k)$ is odd by induction on k, because $\mathcal{W}(1,1)=\mathcal{W}(1,2)=1$. We ignore if also (5) or even the other congruences admit such an easy combinatoric proof.

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 (3)-(4). 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 (4) we conclude that

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

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.

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

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 (3) 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 (3) 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 $\lfloor\frac{l-2}{2}\rfloor = l'-1$. □

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

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

Proof. By Lemma 3 we must prove that

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

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

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

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

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

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

$$\binom{4k'+3}{4l'+1}+\binom{2k'+1}{2l'}=4\delta_{\substack{k',l'\text{ even}\\ l'/2\preceq k'/2}}. \tag{9}$$

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

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

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

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

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. □

Now we study the behavior of

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

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

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

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 (3) 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 pairs $a, a+1$, 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 (3) 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 $\{s\colon s-1 \preceq k-l-2\}$. 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 (3) 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 have 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 the 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.

□

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 $l\leq k-3$. We have proved the claim for $k=3$, therefore we can assume, by induction on k, that the claim holds up to $k-1$. The recursive identity in (1c) and the inductive hypothesis give $M_{k,l}=\mathcal{F}_{k,l}+4\mathcal{G}_{k,l}$ so that the congruence we must prove becomes

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

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

Acknowledgements. The authors thank the anonymous referee for his/her careful reading and comments which have improved the final presentation of this paper.

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] S. Even and A. Lempel, *Generation and enumeration of all solutions of the characteristic sum condition*, Information and Control **21** (1972), 476–482.

[4] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54** (1947), 589–592.

[5] 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.

[6] 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.

[7] G. S. Kazandzidis, *Congruences on the binomial coefficients*, Bull. Soc. Math. Grèce (N.S.) **9** (1968), no. 1, 1–12.

[8] 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.

[9] G. Molteni, *Cancellation in a short exponential sum*, J. Number Theory **130** (2010), no. 9, 2011–2027.

[10] ———, *Representation of a* 2*-power as sum of k* 2*-powers: bounds for the asymptotic behavior*, Int. J. Number Theory **8** (2012), no. 8, 1923–1963.

(Giorgilli) 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

(G. Molteni) Dipartimento di Matematica, Università di Milano, via Saldini 50, I-20133 Milano, Italy

E-mail address: giuseppe.molteni1@unimi.it