On quotients of values of Euler's function on the Catalan numbers

Bojan Bašić

Department of Mathematics and Informatics, University of Novi Sad,

Trg Dositeja Obradovića 4, 21000 Novi Sad, Serbia

bojan.basic@dmi.uns.ac.rs

Abstract

In a recent work, Luca and Stănică examined quotients of the form $\frac{\varphi(C_m)}{\varphi(C_n)}$, where φ is Euler's totient function and $C_0, C_1, C_2 \dots$ is the sequence of the Catalan numbers. They observed that the number 4 (and analogously $\frac{1}{4}$) appears noticeably often as a value of these quotients. We give an explanation of this phenomenon, based on Dickson's conjecture. It turns out not only that the value 4 is (in a certain sense) special in relation to the quotients $\frac{\varphi(C_{n+1})}{\varphi(C_n)}$, but also that the value 4^k has similar "special" properties with respect to the quotients $\frac{\varphi(C_{n+k})}{\varphi(C_n)}$, and in particular we show that Dickson's conjecture implies that, for each k, the number 4^k appears infinitely often as a value of the quotients $\frac{\varphi(C_{n+k})}{\varphi(C_n)}$.

Mathematics Subject Classification (2010): 11A25, 11N32, 11N37, 11B65, 11A63

Keywords: Catalan numbers, Euler's function, totient, Dickson's conjecture

1 Introduction

A well-known Carmichael's conjecture [4] states that for each positive integer n there is a different positive integer m such that $\varphi(m) = \varphi(n)$, where φ is Euler's totient function. Though there are some results related to this conjecture—for example, it is known that a counterexample, if exists, must

be greater than $10^{10^{10}}$, and that in that case there are infinitely many counterexamples [8]; it is known that if there exists an integer n such that for each prime p for which $p-1 \mid \varphi(n)$ we have $p^2 \mid n$, then n is a counterexample to Carmichael's conjecture [13]; it is known that every positive integer greater than 1 is a multiplicity of some value of φ [9] etc.—but the solution to Carmichael's conjecture seems out of reach.

Instead of studying the equality of values of φ, this line of research can be generalized by considering the quotients of the values of φ. In a recent work [10], Luca and Stănică did this with a restriction of the domain to the Catalan numbers $C_0, C_1, C_2 \ldots$; in other words, they examined quotients of the form $\frac{\varphi(C_m)}{\varphi(C_n)}$. They observed that the number 4 (and analogously $\frac{1}{4}$) appears noticeably often as a value of these quotients. In this work we give an explanation of this phenomenon, based on Dickson's conjecture. Furthermore, it turns out not only that the value 4 is (in a certain sense) special in relation to the quotients $\frac{\varphi(C_{n+1})}{\varphi(C_n)}$, but also that the value 4^k has similar "special" properties with respect to the quotients $\frac{\varphi(C_{n+k})}{\varphi(C_n)}$, and in particular we show that Dickson's conjecture implies that, for each k, the number 4^k appears infinitely often as a value of the quotients $\frac{\varphi(C_{n+k})}{\varphi(C_n)}$.

The paper is organized as follows. In Section 2 we state Dickson's conjecture and prove two lemmas that will be useful later. In Section 3 we consider the quotient $\frac{\varphi(C_{n+1})}{\varphi(C_n)}$, where we show that for all integers n of a certain, arguably quite general form, we have the equality $\frac{\varphi(C_{n+1})}{\varphi(C_n)} = 4$; results of Luca and Stănică on this topic are, as is to be shown, two special cases of this theorem. Section 4 is devoted to quotients of the form $\frac{\varphi(C_{n+k})}{\varphi(C_n)}$. Finally, in the Appendix given at the end we collect some results, needed during the work, on divisibility of the Catalan numbers by primes and prime powers.

2 Preliminaries

Dickson's conjecture [5] generalizes Dirichlet's theorem of primes in arithmetic progressions and implies many interesting results such as the infinitude of twin primes, the infinitude of Sophie Germain primes, the infinitude of composite Mersenne numbers etc. (and, needless to say, its proof seems to be hopelessly beyond reach).

Dickson's Conjecture. *Let $P_i(x) = a_i x + b_i$ for $1 \leqslant i \leqslant k$, where $a_i, b_i \in \mathbb{Z}$ and $a_i \geqslant 1$. Then there are infinitely many positive integers x such that*

$P_1(x), P_2(x), \ldots, P_k(x)$ are all primes, unless there exists a prime number p such that for each $x \in \mathbb{Z}$ at least one of $P_1(x), P_2(x), \ldots, P_k(x)$ is divisible by p.

The following lemma give two sufficient conditions (which will be enough for our needs) for the conditions from Dickson's conjecture to be satisfied.

Lemma 1. *a) Let $P_i(x) = a_i x + 1$ for $1 \leqslant i \leqslant k$. Then the polynomials $P_1, P_2, \ldots, P_k$ satisfy the conditions from Dickson's conjecture.*

b) Let $P_i(x) = a_i x + b_i$ for $1 \leqslant i \leqslant k$. If each a_i is coprime to each b_j, and each prime factor less than or equal to k divides some a_i, then the polynomials $P_1, P_2, \ldots, P_k$ satisfy the conditions from the Dickson's conjecture.

Proof. a) Let p be a given prime number. Then whenever x is a multiple of p we have that none of $P_1(x), P_2(x), \ldots, P_k(x)$ are divisible by p.

b) Let p be a given prime number. Assume first that $p \nmid b_i$ for each i. Then whenever x is a multiple of p we have that none of $P_1(x), P_2(x), \ldots, P_k(x)$ are divisible by p.

Let now $p \mid b_{i_0}$ for some i_0. Then $p \nmid a_i$ for each i. We claim that there is a residue class modulo p such that for each x from that residue class none of $P_1(x), P_2(x), \ldots, P_k(x)$ are divisible by p. Note first that, since $p \nmid a_i$ for each i, we have $p > k$. Now, the polynomial $P_1(x)P_2(x)\cdots P_k(x) \bmod p$ is of degree exactly k in $\mathbb{Z}_p[x]$ (because $p \nmid a_1 a_2 \cdots a_k$), and since $p > k$, there exists $x \in \mathbb{Z}_p$ that is not a root of this polynomial. ■

We shall also need the following lemma.

Lemma 2. *If coprime integers m and n satisfy the equality*

$$\frac{m}{\varphi(m)} = \frac{n}{\varphi(n)},$$

then $m = n = 1$.

Proof. The assertion follows by noting that the largest prime factor of the numerator of $\frac{n}{\varphi(n)}$ (as a fraction in lowest terms) is exactly the largest prime factor of n. ■

Finally, for the end of the list of the necessary prerequisites, by $\mathrm{rad}(n)$ we denote the product of the distinct prime factors of n (that is, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime factorization of n, then $\mathrm{rad}(n) = p_1 p_2 \cdots p_k$), and by $\langle a_l, a_{l-1}, \ldots, a_1, a_0 \rangle_b$ we denote the digits expansion of n in the base b (that is, $n = \sum_{i=0}^{l} a_i b^i$ and $0 \leqslant a_i < b$ for each i).

3 The quotient $\frac{\varphi(C_{n+1})}{\varphi(C_n)}$

Let us first recall Theorem 1.1 from [10].

Theorem 3. *The equality*

$$\varphi(C_{n+1}) = 4\varphi(C_n)$$

holds in each of the following two instances:

(i) $n = 2p-2$, *where* $p \geqslant 5$ *is a prime such that* $q = 4p-3$ *is also a prime;*

(ii) $n = 3p-2$, *where* $p > 5$ *is a prime such that* $q = 2p-1$ *is also a prime.*

The theorem cited above is actually a special case of the following more general theorem.

Theorem 4. *Let an integer* u, $u \geqslant 2$, *be given, and let* p, $p \geqslant 2u+1$, *be a prime such that* $2u-3 \mid 2up-3$ *and that* $\frac{2up-3}{2u-3}$ *is also a prime. Then for* $n = up-2$ *the equality*

$$\varphi(C_{n+1}) = 4\varphi(C_n)$$

holds if and only if $\operatorname{rad}(u) \mid C_{n+1}$ *and* $\operatorname{rad}(2(2u-3)) \mid C_n$, *respectively* $\operatorname{rad}(\frac{u}{3}) \mid C_{n+1}$ *and* $\operatorname{rad}(\frac{2(2u-3)}{3}) \mid C_n$, *depending on whether* $3 \nmid u$, *respectively* $3 \mid u$.

Proof. Since $C_n = \frac{\binom{2n}{n}}{n+1}$, we have

$$(n+2)C_{n+1} = 2(2n+1)C_n.$$

Let u and p be as in the statement, and let $q = \frac{2up-3}{2u-3}$ (recall that q is also a prime number). Putting $n = up-2$ (then $2n+1 = 2(up-2)+1 = 2up-3 = (2u-3)q$) in the previous equality gives

$$upC_{n+1} = 2(2u-3)qC_n.$$

Put $\eta = 1$ if $3 \nmid u$ and $\eta = 3$ otherwise. Note that, if $3 \mid u$, then also $3 \mid 2u-3$. From the previous equality we get

$$\frac{u}{\eta}pC_{n+1} = 2\frac{2u-3}{\eta}qC_n. \tag{1}$$

Let c be the product of those prime factors of $\frac{u}{\eta}p$ that do not divide C_{n+1}. Then it is not hard to see

$$\varphi\left(\frac{u}{\eta}pC_{n+1}\right) = \varphi(c)\frac{up}{\eta c}\varphi(C_{n+1}). \tag{2}$$

In a similar manner, if d is the product of those prime factors of $2\frac{2u-3}{\eta}q$ that do not divide C_n, we have

$$\varphi\left(2\frac{2u-3}{\eta}qC_n\right) = \varphi(d)\frac{2(2u-3)q}{\eta d}\varphi(C_n). \tag{3}$$

By (1), (2) and (3), we now have

$$\frac{\varphi(C_{n+1})}{\varphi(C_n)} = \frac{c\varphi(d)2(2u-3)q}{d\varphi(c)up}. \tag{4}$$

Note that, since $u \leqslant \frac{p-1}{2}$ and $n+2 = up = \langle u, 0\rangle_p$, by Theorem 9 we have $p \nmid C_{n+1}$ (that is, $p \mid c$). Let us now show $q \nmid C_n$. We first show $n+1 = \langle u-2, \frac{q+1}{2}\rangle_q$. Using $q = \frac{2up-3}{2u-3}$, it is straightforward to verify

$$(u-2)q + \frac{q+1}{2} = up - 1 = n+1, \tag{5}$$

and therefore it is enough to prove $u-2 \leqslant q-1$ (that is, that $u-2$ is a digit in the base q). We shall prove more: $u-2 \leqslant \frac{q-1}{2}$, which by Theorem 9 immediately leads to $q \nmid C_n$. We have

$$q - 1 = \frac{2up-3}{2u-3} - 1 = \frac{2u(p-1)}{2u-3} \geqslant \frac{2u\cdot 2u}{2u-3} = \frac{4u^2}{2u-3}. \tag{6}$$

Therefore, it is enough to prove $\frac{2u^2}{2u-3} \geqslant u-2$. We calculate

$$\frac{2u^2}{2u-3} - (u-2) = \frac{2u^2 - 2u^2 + 4u + 3u - 6}{2u-3} = \frac{7u-6}{2u-3}. \tag{7}$$

The obtained expression is clearly positive, which proves the claim.

Therefore, $c = pc'$ and $d = qd'$ (and, of course, $p \nmid c'$, $q \nmid d'$). The expression (4) reduces to

$$\begin{aligned}\frac{\varphi(C_{n+1})}{\varphi(C_n)} &= \frac{pc'\varphi(qd')2(2u-3)q}{qd'\varphi(pc')up} = \frac{c'\varphi(qd')2(2u-3)}{d'\varphi(pc')u} \\ &= \frac{c'\varphi(q)\varphi(d')2(2u-3)}{d'\varphi(p)\varphi(c')u} = \frac{c'(q-1)\varphi(d')2(2u-3)}{d'(p-1)\varphi(c')u} \\ &= \frac{c'\frac{2u(p-1)}{2u-3}\varphi(d')2(2u-3)}{d'(p-1)\varphi(c')u} = \frac{4c'\varphi(d')}{d'\varphi(c')}\end{aligned} \tag{8}$$

(during this evaluation we used the equality $q-1 = \frac{2u(p-1)}{2u-3}$, obtained in (6)).

We claim that c' and d' are coprime. Note that $c' \mid \frac{u}{\eta}$ and $d' \mid 2\frac{2u-3}{\eta}$. Therefore,

$$\mathrm{GCD}(c', d') \mid 4\frac{u}{\eta} - 2\frac{2u-3}{\eta} = \frac{6}{\eta}. \tag{9}$$

We first note that c' is odd: indeed, since $2 \mid C_{n+1}$ (which follows by Theorem 8, given the fact that $(n+1)+1 = n+2 = up$, which is clearly not a power of 2), we have $2 \nmid c$, and therefore also $2 \nmid c'$. Therefore, $\mathrm{GCD}(c', d')$ is odd. Now, if $\eta = 1$, then $3 \nmid u$, and therefore neither c' nor d' is divisible by 3; on the other hand, if $\eta = 3$, then (9) gives $\mathrm{GCD}(c', d') \mid 2$. In both cases, together with the conclusion that $\mathrm{GCD}(c', d')$ is odd, we obtain $\mathrm{GCD}(c', d') = 1$, which was to be proved.

We are now ready to finish the proof. By (8) we get $\varphi(C_{n+1}) = 4\varphi(C_n)$ if and only if $\frac{c'}{\varphi(c')} = \frac{d'}{\varphi(d')}$, and since c' and d' are coprime, by Lemma 2 this occurs if and only if $c' = d' = 1$, that is, $c = p$ and $d = q$. By the definition of c, we have that $c = p$ holds if and only if there is no prime factor of $\frac{u}{\eta}p$, apart from p, that does not divide C_{n+1}; by the fact that $p \nmid \frac{u}{\eta}$ (which follows from $p \geqslant 2u+1 > \frac{u}{\eta}$), this is equivalent to

$$\mathrm{rad}\left(\frac{u}{\eta}\right) \mid C_{n+1}.$$

In a similar manner, we have that $d = q$ is equivalent to

$$\mathrm{rad}\left(\frac{2(2u-3)}{\eta}\right) \mid C_n$$

(the only thing that might need explanation here is why $q \nmid \frac{2u-3}{\eta}$, which follows from $q = \frac{2up-3}{2u-3} > \frac{2up-3p}{2u-3} = p \geqslant 2u+1 > \frac{2u-3}{\eta}$). The proof is thus completed. ■

Note. Note that for $u = 2$ in Theorem 4 the condition from the end reduces to $\mathrm{rad}(2) \mid C_{n+1}$ and $\mathrm{rad}(2) \mid C_n$, that is, $2 \mid C_{n+1}$ and $2 \mid C_n$. The first condition is always satisfied since $(n+1)+1 = n+2 = 2p$, which is not a power of 2. The second condition is also always satisfied, since $n+1 = 2p-1$, which, being an odd number, cannot be a power of 2. Therefore, Theorem 3(i) is indeed a special case of Theorem 4 for $u = 2$.

In a similar manner, putting $u = 3$ in Theorem 4 reduces the considered condition to $\mathrm{rad}(1) \mid C_{n+1}$ (which is trivially satisfied) and $\mathrm{rad}(2) \mid C_n$, that is, $2 \mid C_n$. As shown during the proof of Theorem 3 in [10], this is always satisfied, since otherwise we would have $n = 2^a - 1$ where a is odd (because $3 \mid n+2 = 2^a+1$), $p = \frac{n+2}{3} = \frac{2^a+1}{3}$, and then $q = 2p-1 = \frac{2^{a+1}-1}{3} = \frac{(2^{\frac{a+1}{2}}-1)(2^{\frac{a+1}{2}}+1)}{3}$, which cannot be a prime number since $2^{\frac{a+1}{2}}-1, 2^{\frac{a+1}{2}}+1 > 3$. Therefore, Theorem 3(ii) is indeed a special case of Theorem 4 for $u = 3$.

We now show that, under Dickson's conjecture, prime pairs from the statement of Theorem 4 occur infinitely often for each integer u, $u \geqslant 2$.

Theorem 5. *Let an integer u, $u \geqslant 2$, be given. Then, assuming Dickson's conjecture, there are infinitely many prime numbers p such that $2u-3 \mid 2up-3$ and that $\frac{2up-3}{2u-3}$ is also a prime number.*

Proof. Let us state the condition $2u-3 \mid 2up-3$ in the form $2up \equiv 3 \pmod{2u-3}$, that is,

$$3p \equiv 3 \pmod{2u-3}. \tag{10}$$

This is equivalent to $p \equiv 1 \pmod{\frac{2u-3}{\eta}}$, that is,

$$p = \frac{2u-3}{\eta} i + 1$$

for some $i \in \mathbb{N}_0$, where we again denote $\eta = 1$ if $3 \nmid u$ and $\eta = 3$ otherwise. We then have

$$q = \frac{2up-3}{2u-3} = \frac{2u(\frac{2u-3}{\eta} i + 1) - 3}{2u-3} = \frac{2u}{\eta} i + 1.$$

By Lemma 1a) we obtain that there are infinitely many values of i such that p and q are both primes, which was to be proved. ■

Finally, since for each prime number p almost all Catalan numbers are divisible by p (see Corollary 10), the condition from the end of Theorem 4 is almost always satisfied. Everything said so far explains, at least on an intuitive level, why the value 4 appears so often among the values of the considered quotient.

So far we have analyzed only the equality $\frac{\varphi(C_{n+1})}{\varphi(C_n)} = 4$. In the last part of this section we would like to make some comments on the limitations of the used method, that is, what would be needed in order to analyze the considered equality with 4 replaced by another constant.

Let p be a prime number that satisfies the conditions from Theorem 4. Note that c' is a product of those prime factors of $\frac{u}{\eta}$ that do not divide C_{n+1}, while d' is the product of those prime factors of $2\frac{2u-3}{\eta}$ that do not divide C_n. Therefore, we almost always have $c' = 1$ and $d' = 1$. However, if r is a given prime number, then by Theorem 9 there is still infinitely many indices n such that $r \nmid C_{n+1}$ (respectively $r \nmid C_n$). This is also a good moment to recall the result from [7], which states that for any two given primes r_1 and r_2 there are infinitely many integers n such that $\mathrm{GCD}(\binom{2n}{n}, r_1 r_2) = 1$. But that is not exactly what we need. In order to use the equality (8) to prove the infinitude of some other possible values of $\frac{\varphi(C_{n+1})}{\varphi(C_n)}$, we not only have to show that there are infinitely many indices n such that C_{n+1} (respectively C_n) is not divisible by a given prime (or given primes), but we need infinitely many such indices of the form $up - 2$ (where u is a fixed number, and p takes prime values such that $\frac{2up-3}{2u-3}$ is also a prime). Based on the cited results (more precisely, on a hope that the behavior does not change substantially when restricting the values of n to the given form), we believe that this indeed holds when c' and d' have few prime factors (say, no more than 2 in total).

For the sake of amusement, we tried to find some values of n for $c' = 5$, $d' = 7$ (then $\frac{\varphi(C_{n+1})}{\varphi(C_n)} = \frac{4\cdot 5\cdot \varphi(7)}{7\cdot \varphi(5)} = \frac{30}{7}$) and $u = 40$ (here is why this value of u is chosen: the least value of u that allows $c' = 5$ and $d' = 7$, that is, such that $5 \mid \frac{u}{\eta}$ and $7 \mid 2\frac{2u-3}{\eta}$, is $u = 5$; we intentionally chose the next larger value of u, because for $u = 5$ the required values of n seem to be fairly dense, and we were interested whether we could find any values for a larger u). There are three such values for $p < 10^{11}$: $n = 305\,444\,240\,678$ ($p = 7\,636\,106\,017$ and $q = 7\,933\,616\,641$), $n = 777\,707\,219\,558$ ($p = 19\,442\,680\,489$ and $q = 20\,200\,187\,521$) and $n = 1\,564\,994\,532\,678$ ($p = 39\,124\,863\,317$ and $q = 40\,649\,208\,641$).

Trying to control the divisibility of the Catalan numbers simultaneously

by 3 (or more) primes (which is needed in the cases of c' and d' having more prime factors) is related to the following quite well-known open problem: are there infinitely many values of n such that $\mathrm{GCD}(\binom{2n}{n}, 105) = 1$? It is believed (and suggested by a heuristic) that the answer is yes, and Graham offers \$1,000 to anyone who proves that [11, 3, 15, 12]. For the same question but with 105 replaced by a product of 4 or more different primes, the answer is likely to be negative, but this is also an open problem.

4 The quotient $\frac{\varphi(C_{n+k})}{\varphi(C_n)}$

We now prove a theorem analogous to Theorem 4 for the quotient $\frac{\varphi(C_{n+k})}{\varphi(C_n)}$. Although the statement includes a number of technical restrictions, after this theorem we shall show that, in a certain sense, it is not substantially hard to satisfy these restrictions.

Theorem 6. *Assume that integers $u_1, u_2, \ldots, u_k$ greater than 1 and different primes $p_1, p_2, \ldots, p_k$ are chosen such that:*

- *for each i, $1 \leqslant i \leqslant k$, we have $p_i \geqslant 2u+1$, where $u = \max\{u_1, \ldots, u_k\}$;*
- *$u_1p_1 = u_2p_2 - 1 = u_3p_3 - 2 = \cdots = u_kp_k - k + 1$;*
- *for each i, $1 \leqslant i \leqslant k$, we have $2u_i - 3 \mid 2u_ip_i - 3$ and $\frac{2u_ip_i-3}{2u_i-3}$ is also a prime, and furthermore, all those k primes are different.*

Then for $n = u_1p_1 - 2$ the equality

$$\varphi(C_{n+k}) = 4^k\varphi(C_n)$$

holds if and only if

$$\mathrm{rad}\left(\frac{\prod_{i=1}^k u_i}{\eta}\right) \mid C_{n+k} \quad \text{and} \quad \mathrm{rad}\left(2\frac{\prod_{i=1}^k (2u_i-3)}{\eta}\right) \mid C_n, \tag{11}$$

where $\eta = \mathrm{GCD}\left(\prod_{i=1}^k u_i, \prod_{i=1}^k (2u_i-3)\right)$.

Proof. We have

$$\frac{C_{n+k}}{C_n} = 2^k \prod_{i=1}^{k} \frac{2n+2i-1}{n+i+1},$$

that is,

$$\left(\prod_{i=1}^{k}(n+i+1)\right)C_{n+k}=\left(2^k\prod_{i=1}^{k}(2n+2i-1)\right)C_n.$$

Let $u_1,u_2,\ldots,u_k$ and $p_1,p_2,\ldots,p_k$ be as in the statement, and let $q_i=\frac{2u_ip_i-3}{2u_i-3}$ for $1\leqslant i\leqslant k$ (recall that each q_i is also a prime number). Put $n=u_1p_1-2=u_2p_2-3=\cdots=u_kp_k-k-1$. Then $2n+2i-1=2(u_ip_i-i-1)+2i-1=2u_ip_i-3=(2u_i-3)q_i$. The previous equality then reduces to

$$\left(\prod_{i=1}^{k}u_ip_i\right)C_{n+k}=\left(2^k\prod_{i=1}^{k}(2u_i-3)q_i\right)C_n.$$

Let

$$\eta=\mathrm{GCD}\left(\prod_{i=1}^{k}u_i,\prod_{i=1}^{k}(2u_i-3)\right).$$

We therefore have

$$\frac{u_1u_2\cdots u_k}{\eta}p_1p_2\cdots p_kC_{n+k}=2^k\frac{\prod_{i=1}^{k}(2u_i-3)}{\eta}q_1q_2\cdots q_kC_n.$$

Denote by c the product of those prime factors of $\frac{u_1u_2\cdots u_k}{\eta}p_1p_2\cdots p_k$ that do not divide C_{n+k}, and denote by d the product of those prime factors of $2^k\frac{\prod_{i=1}^{k}(2u_i-3)}{\eta}q_1q_2\cdots q_k$ that do not divide C_n. It follows

$$\varphi\left(\frac{u_1u_2\cdots u_k}{\eta}p_1p_2\cdots p_kC_{n+k}\right)=\varphi(c)\frac{u_1u_2\cdots u_kp_1p_2\cdots p_k}{\eta c}\varphi(C_{n+k})$$

and

$$\varphi\left(2^k\frac{\prod_{i=1}^{k}(2u_i-3)}{\eta}q_1q_2\cdots q_kC_n\right)=\varphi(d)\frac{2^k\prod_{i=1}^{k}(2u_i-3)\prod_{i=1}^{k}q_i}{\eta d}\varphi(C_n),$$

that is,

$$\frac{\varphi(C_{n+k})}{\varphi(C_n)}=\frac{c\varphi(d)2^k\left(\prod_{i=1}^{k}(2u_i-3)\right)q_1q_2\cdots q_k}{d\varphi(c)u_1u_2\cdots u_kp_1p_2\cdots p_k}. \tag{12}$$

We now claim that for each i, $1\leqslant i\leqslant k$, we have $p_i\mid c$. It is enough to prove $p_i\nmid C_{n+k}$. Since $n+k+1=u_ip_i+k-i=\langle u_i,k-i\rangle_{p_i}$, the claim follows by

Theorem 9 and the inequalities $u_i \leqslant \frac{p_i-1}{2}$ and $k-i \leqslant \frac{p_i+1}{2}$. We further claim that for each i, $1 \leqslant i \leqslant k$, we have $q_i \mid d$. From $\langle u_i-2, \frac{q_i+1}{2}\rangle_{q_i} = u_i p_i - 1 = n+i$ (verified in the same way as (5)) we get $n+1 = \langle u_i-2, \frac{q_i-2i+3}{2}\rangle_{q_i}$, where the left-hand digit is positive as in (6) and (7), while the right-hand digit is nonnegative because of

$$q_i - 2i + 3 = \frac{2u_i p_i - 3}{2u_i - 3} - 2i + 3 \geqslant \frac{2u_i(2i-1)-3}{2u_i-3} - 2i + 3 = \frac{2(2u_i + 3i - 6)}{2u_i - 3};$$

therefore, by Theorem 9 we conclude $q_i \nmid C_n$ and thus $q_i \mid d$. We now write $c = p_1 p_2 \cdots p_k c'$ and $d = q_1 q_2 \cdots q_k d'$, and put this into (12), which leads to

$$\begin{aligned}\frac{\varphi(C_{n+k})}{\varphi(C_n)} &= \frac{c'\varphi(q_1 q_2 \cdots q_k d') 2^k \prod_{i=1}^k (2u_i - 3)}{d'\varphi(p_1 p_2 \cdots p_k c') u_1 u_2 \cdots u_k} \\ &= \frac{2^k c'\varphi(d')}{d'\varphi(c')} \prod_{i=1}^k \frac{(q_i-1)(2u_i-3)}{(p_i-1)u_i} \\ &= \frac{2^k c'\varphi(d')}{d'\varphi(c')} \prod_{i=1}^k \frac{\frac{2u_i(p_i-1)}{2u_i-3}(2u_i-3)}{(p_i-1)u_i} = \frac{4^k c'\varphi(d')}{d'\varphi(c')}\end{aligned} \tag{13}$$

Since $n+k+1 = u_k p_k$, which is clearly not a power of 2, by Theorem 8 we get $2 \mid C_{n+k}$, and hence $2 \nmid c'$. Since $c' \mid \frac{u_1 u_2 \cdots u_k}{\eta}$ and $d' \mid 2^k \frac{\prod_{i=1}^k (2u_i-3)}{\eta}$, and since c' is odd, by the definition of η we obtain that c' and d' are coprime. Therefore, since $\varphi(C_{n+k}) = 4^k \varphi(C_n)$ if and only if $\frac{c'}{\varphi(c')} = \frac{d'}{\varphi(d')}$, by the coprimality of c' and d' and Lemma 2 we conclude that this happens if and only if $c' = 1$ and $d' = 1$, that is, $c = p_1 p_2 \cdots p_k$ and $d = q_1 q_2 \cdots q_k$. The first condition holds if and only if all prime factors of $\frac{u_1 u_2 \cdots u_k}{\eta}$, except possibly $p_1, p_2, \ldots, p_k$, divide C_{n+k}; since neither of $p_1, p_2, \ldots, p_k$ divides $\frac{u_1 u_2 \cdots u_k}{\eta}$ (because p_i is greater than each of $u_1, u_2, \ldots, u_k$, and thus divides none of them), this is further equivalent to

$$\operatorname{rad}\left(\frac{u_1 u_2 \cdots u_k}{\eta}\right) \mid C_{n+k}.$$

In a similar manner, the second condition is equivalent to

$$\operatorname{rad}\left(2\frac{\prod_{i=1}^k (2u_i-3)}{\eta}\right) \mid C_n$$

(the inequality $q_i = \frac{2u_ip_i-3}{2u_i-3} > \frac{2u_ip_i-3p_i}{2u_i-3} = p_i \geqslant \frac{2u_i-3}{\eta}$ is relevant here), which completes the proof. ■

Note. As we can see, the core of the previous theorem are the equalities $n+2 = u_1p_1$, $n+3 = u_2p_2$, …, $n+k+1 = u_kp_k$ and $2n+1 = (2u_1-3)q_1$, $2n+3 = (2u_2-3)q_2$, …, $2n+2k-1 = (2u_k-3)q_k$, where, thanks to the coefficients $2u_i-3$, it turns out that q_i-1 is a "nice" rational multiple of p_i-1, namely,

$$q_i - 1 = \frac{2n+2i-1}{2u_i-3} - 1 = \frac{2(u_ip_i-i-1)+2i-2u_i+2}{2u_i-3} = \frac{2u_i}{2u_i-3}(p_i-1).$$

It can be asked whether a different pairing of q_i's with p_i's—that is, making each q_i a "nice" rational multiple of $p_{\sigma(i)}-1$, where σ is a permutation of $\{1,2,\ldots,n\}$—can lead to another value of the considered quotient instead of 4^k. And unfortunately, although the pairing can be made in a different manner, we do not get another value instead of 4^k. For example, let us see how to pair q_1 with p_2, q_2 with p_1 and q_i with p_i for other i. We need the conditions $2n+1 = v_1q_1$ and $2n+3 = v_2q_2$ (and $2n+2i-1 = (2u_i-3)q_i$ for $i \geqslant 3$), where we shall now choose the values v_1 and v_2 in a suitable manner. We have

$$q_1 - 1 = \frac{2n+1}{v_1} - 1 = \frac{2(u_2p_2-3)+1}{v_1} - 1 = \frac{2u_2p_2-5-v_1}{v_1};$$

therefore, in order to make p_2-1 a factor of the expression above, we choose $v_1 = 2u_2-5$. In a similar manner we find out that the choice $v_2 = 2u_1-1$ is adequate. In this case, the product from (13) is replaced by

$$\frac{(q_1-1)(2u_2-5)}{(p_2-1)u_2} \cdot \frac{(q_2-1)(2u_1-1)}{(p_1-1)u_1} \cdot \prod_{i=3}^{k} \frac{(q_i-1)(2u_i-3)}{(p_i-1)u_i},$$

which evaluates to 2^k, that is, the same value as in (13).

As we shall now see, relying on Theorem 6, Dickson's conjecture implies that for each positive integer k there are infinitely many positive integers n such that $\frac{\varphi(C_{n+k})}{\varphi(C_n)} = 4^k$. We shall prove this by fixing $u_1 = 2$, $u_2 = 3$, …, $u_k = k+1$, and showing that the conditions from Theorem 6 can be satisfied in infinitely many cases. We would just like to note that there is nothing very special about those fixed values. In fact, by suitable changes in

the proof that is about to follow the same result can be shown to hold for many other values fixed for u_i (though this may be much more technically challenging), and in particular, if any *consecutive* positive integers are fixed for $u_1, u_2, \ldots, u_k$, the required changes are fairly simple.

Theorem 7. *Let a positive integer k be given. Assuming Dickson's conjecture, there are infinitely many positive integers n such that*

$$\frac{\varphi(C_{n+k})}{\varphi(C_n)} = 4^k. \tag{14}$$

Proof. Fix $u_i = i + 1$ for $1 \leqslant i \leqslant k$. We need to find n (actually, infinitely many of them) such that

$$n = u_1 p_1 - 2 = u_2 p_2 - 3 = \cdots = u_k p_k - k - 1, \tag{15}$$

where $p_1, p_2, \ldots, p_k$ are different primes. Further, we should also have $2u_i - 3 \mid 2u_i p_i - 3$, that is, $2i - 1 \mid 2n + 2i - 1$ (which is equivalent to $2i - 1 \mid n$), and $\frac{2n+2i-1}{2i-1}$ should be different primes. Because of (15), we conclude $i+1 = u_i \mid n$, which together with the previous set of divisibility conditions gives $C \mid n$, where $C = \mathrm{LCM}(2, 3, \ldots, k+1, 1, 3, 5, \ldots, 2k-1)$. Let

$$M = \mathrm{LCM}\left(C^2, \prod_{\substack{p \text{ prime} \\ p \leqslant 2k}} p\right).$$

Before proceeding to show how to find such n and the corresponding primes, we shall see how to make sure that, for a chosen n, the conditions (11) are satisfied. Let $s_1, s_2, \ldots, s_h$ be all the prime divisors of either of $\mathrm{rad}\left(\frac{\prod_{i=1}^k u_i}{\eta}\right)$ or $\mathrm{rad}\left(2\frac{\prod_{i=1}^k (2u_i-3)}{\eta}\right)$, and for each i, $1 \leqslant i \leqslant h$, let α_i be the smallest positive integer such that $s_i^{\alpha_i+1} \nmid M$ and $s_i^{\alpha_i} > k+1$ (note that, since clearly $s_i \mid M$, we have $\alpha_i \geqslant 1$, that is, α_i is indeed positive). We impose the congruence $n \equiv \frac{s_i+1}{2} s_i^{\alpha_i} \pmod{s_i^{\alpha_i+1}}$; as an exception, if $s_i = 2$, we then impose the congruence $n \equiv 0 \pmod{2^{\alpha_i+1}}$ instead. Finally, we impose one more congruence: $n \equiv 0 \pmod{M'}$, where M' is the greatest divisor of M coprime to $s_1 s_2 \cdots s_h$. Note that, since $s_i^{\alpha_i} \mid n$, all these congruences are compatible with the condition $M \mid n$ (because the greatest power of s_i that divides M is not greater than $s_i^{\alpha_i}$), and thus also compatible with $C \mid n$.

Now, since the last $\alpha_i + 1$ digits of n in the base s_i form the number $\frac{s_i+1}{2}s_i^{\alpha_i}$, and since $\frac{s_i+1}{2}s_i^{\alpha_i} + k + 1 < \frac{s_i+1}{2}s_i^{\alpha_i} + s_i^{\alpha_i} = \frac{s_i+3}{2}s_i^{\alpha_i}$, the digit at the position $\alpha_i + 1$ from the right in the number $n + k + 1$ written in the base s_i is $\frac{s_i+1}{2}$, which by Theorem 9 implies $s_i \mid C_{n+k}$; for the same reason, $s_i \mid C_n$ (if $s_i = 2$, then the observed digit is 0 instead of $\frac{s_i+1}{2}$, and then the same conclusion holds by Theorem 8). By the Chinese remainder theorem, the imposed set of congruences has infinitely many solutions, and all of them are of the form $n = Qx + L$ for some constants Q and L (where, by construction, $M \mid Q$ and $\mathrm{rad}(M) = \mathrm{rad}(Q)$, and furthermore $M \mid L$, all of which will be needed soon).

Rewritting the equation (15), we obtain

$$p_i = \frac{n+i+1}{u_i} = \frac{Q}{i+1}x + \frac{L}{i+1} + 1.$$

We need to find infinitely many x such that all these values (for $1 \leqslant i \leqslant k$) are different primes, and that all the values $\frac{2n+2i-1}{2i-1} = \frac{2Q}{2i-1}x + \frac{2L}{2i-1} + 1$ (for $1 \leqslant i \leqslant k$) are different primes. However, note that these $2k$ polynomials satisfy the conditions from Lemma 1b) (indeed, by the choice of M and the relations $M \mid Q$, $\mathrm{rad}(M) = \mathrm{rad}(Q)$ and $M \mid L$ we directly get $\mathrm{GCD}(\frac{Q}{i+1}, \frac{L}{j+1}) > 1$ etc., which implies that $\frac{Q}{i+1}$ and $\frac{L}{j+1} + 1$ are coprime, and similarly for the other three pair types), and thus these $2k$ values are indeed simultaneously prime for infinitely many values of x. It is obvious that, for each such x, no two of p_i can be equal, and no two of the other k primes can be equal. ■

Note. By a quantitative version of Dickson's conjecture (known, in its very general form, under the name Bateman-Horn conjecture), the number of values x from the interval $[1, z]$ such that the $2k$ polynomials from the preceding proof are simultaneously prime at the point x is of order at least $\int_2^z \frac{dt}{(\ln t)^{2k}}$ (or, which is asymptotically the same, $\frac{z}{(\ln z)^{2k}}$). Therefore, we also have a (conjectured) lower bound for the number of values n such that (14) holds.

Appendix: On divisibility of the Catalan numbers by primes

In this section we give various theorems about divisibility of the Catalan numbers by primes and prime powers, needed in the previous sections.

We give the first theorem without proof (for the proof see, for example [14], and more different proofs are given in [1]).

Theorem 8. *The number C_n is odd if and only if $n+1$ is a power of 2.*

We need a similar criterion for divisibility of C_n by odd primes. Our proof of it will rely on the following (well-known) theorem. (We would like to add that, since the criterion that is about to follow is quite elegant and not hard to prove, it seems like it certainly has already appeared somewhere in the literature. However, our search of the literature in order to find it was unsuccessful. There are some criteria of divisibility of C_n by odd primes in [2], but they are not practical for our purpose here, and there is also a very recent criterion from [6, Corollary 18], that bears a resemblance to our Theorem 9, but we still find our criterion more convenient for the present work.)

Kummer's theorem. *Let a prime p and nonnegative integers n and m be given, $n \geqslant m$. Then the largest integer α such that $p^\alpha \mid \binom{n}{m}$ is equal to the number of carries when m is added to $n-m$ in the base p.*

And here is the announced criterion.

Theorem 9. *Let p be an odd prime number. Then $p \nmid C_n$ if and only if the rightmost digit of the number $n+1$ in the base p is less than or equal to $\frac{p+1}{2}$, and all the other digits are less than or equal to $\frac{p-1}{2}$.*

Proof. First note that n satisfies the digit condition from the statement if and only if n written in the base p is of one of the following two forms: (i) all the digits are less than or equal to $\frac{p-1}{2}$; or (ii) the rightmost α digits (for some α) are $p-1$, the digit immediately left of them is less than or equal to $\frac{p-3}{2}$, and all the other digits are less than or equal to $\frac{p-1}{2}$. In the rest of the proof we shall use these conditions instead of the ones from the statement.

($\Rightarrow$): Assume $p \nmid C_n$. This implies that either $p \nmid \binom{2n}{n}$, or p appears with the same power in $\binom{2n}{n}$ as in $n+1$. In the first case, by Kummer's theorem we conclude that there must not be any carries when n is added to n in the base p, which immediately implies that n is of the form (i). Assume now the second case. If the considered power of p is p^α, then because of $p^\alpha \mid n+1$ we conclude that the rightmost α digits of n in the base p are $p-1$. Clearly, in each of these positions there will be a carry when n is added to n in the base p, which gives a total of α carries so far. However, since $p^{\alpha+1} \nmid \binom{2n}{n}$, by Kummer's theorem there must not be any more carries apart from those α, which implies that n is of the form (ii).

($\Leftarrow$): This direction is easier. If n is of the form (i), there are no carries, and therefore $p \nmid \binom{2n}{n}$ (and thus $p \nmid C_n$). If n is of the form (ii), then there are exactly α carries (precisely those in the rightmost α positions), and $n+1$ ends with α zeros, that is, is divisible by p^α, which again implies $p \nmid C_n$. ■

Finally, the following corollary is an immediate consequence of the theorem above.

Corollary 10. *For a given $z \in \mathbb{R}$, the number of the values n less than z such that C_n is not divisible by a given prime p is at most $O_p(z^{\log_p \frac{p+1}{2}})$, where the multiplicative constant implied by the Landau symbol O_p depends only on p.*

Acknowledgments

The author would like to thank the anonymous referee for valuable comments, which helped to improve the content of the paper.

The research was supported by the Ministry of Science and Technological Development of Serbia (project 174006) and by the Provincial Secretariat for Science and Technological Development, Autonomous Province of Vojvodina (project "Ordered and related structures and applications").

References

[1] R. Alter & T. B. Curtz, On binary non-associative products and their relation to a classical problem of Euler, *Comment. Math. Prace Mat.* **17** (1973), 1–8.

[2] R. Alter & K. K. Kubota, Prime and Prime Power Divisibility of Catalan Numbers, *J. Combinatorial Theory Ser. A* **15** (1973), 243–256.

[3] D. Berend & J. E. Harmse, On some arithmetical properties of middle binomial coefficients, *Acta Arith.* **84** (1998), 31–41.

[4] R. D. Carmichael, Note on Euler's φ-function, *Bull. Amer. Math. Soc.* **28** (1922), 109–110.

[5] L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, *Messenger of Mathematics* **33** (1904), 155–161.

[6] T. Edgar & M. Z. Spivey, Multiplicative functions, generalized binomial coefficients, and generalized Catalan numbers, *J. Integer Seq.* **19** (2016), Article 16.1.6, 21 pp.

[7] P. Erdős & R. L. Graham & I. Z. Ruzsa & E. G. Straus, On the prime factors of $\binom{2n}{n}$, *Math. Comp.* **29** (1975), 83–92.

[8] K. Ford, The distribution of totients, *Ramanujan J.* **2** (1998), 67–151.

[9] K. Ford, The number of solutions of $\varphi(x) = m$, *Ann. of Math. (2)* **150** (1999), 283–311.

[10] F. Luca & P. Stănică, On the Euler function of the Catalan numbers, *J. Number Theory* **132** (2012), 1404–1424.

[11] R. D. Mauldin & S. M. Ulam, Mathematical problems and games, *Adv. in Appl. Math.* **8** (1987), 281–344.

[12] C. Pomerance, Divisors of the middle binomial coefficient, *Amer. Math. Monthly* **122** (2015), 636–644.

[13] C. Pomerance, On Carmichael's conjecture, *Proc. Amer. Math. Soc.* **43** (1974), 297–298.

[14] D. M. Silberger, Occurrences of the integer $(2n-2)!/n!(n-1)!$, *Comment. Math. Prace Mat.* **13** (1969), 91–96.

[15] A. Straub & V. H. Moll & T. Amdeberhan, The p-adic valuation of k-central binomial coefficients, *Acta Arith.* **140** (2009), 31–42.