GCD OF TRUNCATED ROWS IN PASCAL'S TRIANGLE

Gil Kaplan
Department of Mathematics and Computer Science, The Academic College of Tel-Aviv-Yaffo, Tel-Aviv 64044 Israel

Dan Levy
Department of Mathematics and Computer Science, The Academic College of Tel-Aviv-Yaffo, Tel-Aviv 64044 Israel

Received: 12/19/03, Revised: 8/3/04, Accepted: 10/15/04, Published: 10/20/04

Abstract

In this paper we study $\gcd\left(\binom{n}{t}, \binom{n}{t+1}, ..., \binom{n}{n-t}\right)$. By arranging these numbers in a triangle and exploring a local divisiblity property of its elements, we uncover relations among them which lead to an interesting description of their complete prime factorization.

1. Introduction and Main Results

The binomial coefficients are known to have remarkable arithmetic properties. Leading number theorists of the 19th century have discovered many results concerning their values modulo prime powers (an excellent on-line review of such results is [3]). Among these, Kummer's theorem [5] plays a key role. In essence it says that the exact power of a prime p dividing the binomial coefficient $\binom{n}{k}$ is equal to the number of carries occurring in the addition of k and $n-k$. The term "carry" is used to denote "an amount propagated to the current digit position from the digits in the less significant positions"[4] when adding two numbers.

As is well known, some important properties of binomial coefficients can be deduced more easily after arranging them in an infinite table called Pascal's triangle. The first ten rows of Pascal's triangle are given in Table 1. The numbering of rows and columns starts from 0, and increases downwards and rightwards respectively, so that $\binom{n}{k}$ is at the n-th row and k-th column. One can construct Pascal's triangle recursively, row by row, using Pascal's law

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \tag{1}$$

and the boundary conditions $\binom{n}{0} = \binom{n}{n} = 1$. Pascal's triangle is also useful in studying

1									
1	1								
1	2	1							
1	3	3	1						
1	4	6	4	1					
1	5	10	10	5	1				
1	6	15	20	15	6	1			
1	7	21	35	35	21	7	1		
1	8	28	56	70	56	28	8	1	
1	9	36	84	126	126	84	36	9	1

Table 1: First ten rows of Pascal's triangle

arithmetic properties of binomial coefficients. For instance, the triangle obtained from Pascal's triangle by replacing each entry by its residue modulo some fixed prime p, is known to have an interesting self-similar structure [3].

In the present paper we consider the greatest common divisor (gcd) of elements belonging to the same row of Pascal's triangle. More precisely we focus our attention on the following object.

Notation 1 *For any two integers $n \geq 0$ and $0 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor$, let $g(n,t)$ stand for the gcd of the elements in the symmetrically t-truncated n-th row of Pascal's triangle, i.e.,*

$$\begin{aligned} g(n,t) &= \gcd\left(\binom{n}{t}, \binom{n}{t+1}, ..., \binom{n}{n-t}\right) \\ &= \gcd\left(\binom{n}{t}, \binom{n}{t+1}, ..., \binom{n}{\left\lfloor \frac{n}{2} \right\rfloor}\right). \end{aligned}$$

When using the notation above it is understood that $\gcd(x) = x$. Note also that the second equality follows from the well known symmetry property $\binom{n}{k} = \binom{n}{n-k}$ and that t is the number of elements left out on each side of the row.

In fact, we find it useful to view these numbers as entries in another triangle, where n labels the rows and t the columns (as for Pascal's triangle, the numbering of rows and columns starts from 0, and increases downwards and rightwards respectively). We will refer to this triangle as the g-triangle. The first ten rows of the g-triangle are given in Table 2.

The gcd of truncated rows in Pascal's triangle is discussed in a recent paper by Soulé [6]. For each n-th row of Pascal's triangle he defines $b(n)$ to be the minimal value of t for which $g(n, t+1) > 1$. Note that we trivially have:

$$g(n,0) = 1 \ , \ \forall n \geq 0 \tag{2}$$

so therefore $b(n)$ is a non-negative integer. Soulé attributes the following theorem (his Theorem 3) to Granville.

Theorem 2 *(Granville): For $n > 0$, $b(n)$ is the smallest integer of the form $n - p^{\alpha}$ where p^{α} is a prime power less or equal to n. Furthermore, $g(n, b(n)+1) = p$.*

Remark 3 The last part of Theorem 2, i.e., $g(n, b(n)+1) = p$, is not part of the original statement of the theorem, as given in [6]. It follows naturally from our results as will be shown later.

For example, examining Table 2, we see that $b(n) = 0$ for all $0 \leq n \leq 8$, except for $n = 6$ for which $b(6) = 1$. Indeed, 6 is the only positive number in this range which is not a prime power (5 being the closest prime power to 6 from below). The equality $g(n, b(n)+1) = p$ can also be checked directly for $0 \leq n \leq 8$ from Table 2.

Due to Theorem 2, one can use known results on the density of the prime numbers in order to estimate $b(n)$. Since the number of primes up to a given n is of the order $\frac{n}{\log n}$, we can expect typical values of $b(n)$ to be of the order $\log n$. However, for the moment, $b(n) \leq n^{0.525}$ for all large enough n seems to be the best available upper bound on $b(n)$ (see [1]).

We now summarize our results on the gcd of truncated rows in Pascal's triangle. In addition to the g-triangle we introduce (see Notation 6) a second triangle which we term the h-triangle. Our main result, Theorem 7, exhibits a fascinating property of the h-triangle. Column t of the h-triangle contains the complete list of the prime factors of t. Theorem 9 and the discussion following it show how to locate in the h-triangle the complete list of the prime factors of each of the elements of the g-triangle.

The first theorem calculates the entries of the first non-trivial column of the g-triangle.

Theorem 4 *For all $n \geq 2$ we have:*

$$g(n,1) = \begin{cases} p, & n = p^{\alpha}, \text{ where } p \text{ is a prime and } \alpha \text{ a positive integer,} \\ 1, & \text{otherwise.} \end{cases} \tag{3}$$

The next result exhibits a useful divisibility property of neighboring entries of the g-triangle.

Theorem 5 *Let n and t be two integers such that $n \geq 2$ and $0 \leq t < \left\lfloor \frac{n}{2} \right\rfloor$. Then*

$$\operatorname{lcm}\left(g(n-1,t), g(n,t)\right) \text{ divides } g(n,t+1), \tag{4}$$

where $\operatorname{lcm}(a,b)$ stands for the least common multiple of a and b.

1				
1				
1	2			
1	3			
1	2	6		
1	5	10		
1	1	5	20	
1	7	7	35	
1	2	14	14	70
1	3	6	42	126

Table 2: First ten rows of the g-triangle

2			
3			
2	1		
5	1		
1	1	2	
7	1	1	
2	1	1	1
3	1	1	3

Table 3: First eight rows of the h(n,t) triangle

For example, taking $n = 6$ and $t = 2$ we get $\operatorname{lcm}(10, 5) = 10$ is a divisor of $g(6, 3) = 20$. In order to turn (4) into an equation which can be used to construct the g-triangle recursively, analogous to the way Pascal's law (1) is used to construct Pascal's triangle, we study the following integer quantity.

Notation 6 *For $n \geq 2$ and for $0 \leq t < \left\lfloor \frac{n}{2} \right\rfloor$, let*

$$h(n,t) = \frac{g(n, t+1)}{\operatorname{lcm}(g(n-1,t), g(n,t))}.$$

Again, we view these numbers as entries in a triangle, which will be termed the h-triangle, where $n \geq 2$ labels the rows and $t \geq 0$ the columns (as before, indexing of rows increases downwards and indexing of columns increases rightwards). The first eight rows of this triangle are given in Table 3.

From (2) and (3) it immediately follows that:

$$h(n,0) = \begin{cases} p, & \text{if } n = p^{\alpha} \text{ where } p \text{ is prime and } \alpha \text{ a positive integer} \\ 1, & \text{otherwise} \end{cases} \tag{5}$$

Our main result concerns the other values of $h(n,t)$.

Theorem 7 *Fix $t \geq 1$, and for $t > 1$ let $t = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$ be its primary decomposition. For all $n \geq 4$ such that $t < \left\lfloor \frac{n}{2} \right\rfloor$, if $n - 2t = p_i^{\alpha}$ for some integers $1 \leq i \leq k$ and $1 \leq \alpha \leq \alpha_i$, then $h(n,t) = p_i$. Otherwise $h(n,t) = 1$.*

As an example, take $t = 2$. The only $h(n,2)$ different from 1 is $h(6,2) = 2$.

Remark 8 Theorem 7 implies in particular that $h(n,t)$ is either 1 or a prime, and that for a fixed $t \geq 2$, if we vary n starting from $2t+2$, we get the complete primary decomposition of t in the t-th column of the h-triangle. In fact, it is not hard to prove that the same phenomenon occurs along diagonals: we get the complete primary decomposition of d along the diagonal $\{(i,j) \,|i - j = d\}$. Note also that due to Theorem 7, $h(n,t)$ can be effectively computed directly from the values of n and t (instead of computing it from its defining equation (see Notation 6)). This statement relies on the fact that there is an effective algorithm to determine whether a given integer is a prime power and, if it is, what is the value of this prime (such an algorithm is described, for instance, in [2] (Algorithm 1.7.5.)). So, all one has to do, given a pair (n,t), is to check whether $(n-2t)$ divides t and whether $n - 2t = p^{\alpha}$ for some prime p and for some positive integer α. If both conditions are satisfied, then $h(n,t) = p$. Otherwise $h(n,t) = 1$.

The next theorem shows how to obtain the prime factorization of $g(n,t)$ from the h-triangle.

Theorem 9 *For all $n \geq 2$, $0 \leq t < \left\lfloor \frac{n}{2} \right\rfloor$,*

$$g(n, t+1) = \prod_{(i,j) \in T(n,t)} h(i,j),$$

where $T(n,t)$ is the right-angled isosceles triangle whose corners are $(n-t, 0)$, $(n,0)$, (n,t).

For example, we can compute $g(9,3)$ in the following way ($n = 9$, $t = 2$)

$$\begin{aligned} g(9,3) &= \prod_{(i,j) \in T(9,3)} h(i,j) = \prod_{7 \leq i \leq 9} \prod_{0 \leq j \leq i-7} h(i,j) = \\ &= h(7,0)\, h(8,0)\, h(8,1)\, h(9,0)\, h(9,1)\, h(9,2) = \\ &= 7 \cdot 2 \cdot 1 \cdot 3 \cdot 1 \cdot 1 = 42. \end{aligned}$$

We now collect some simple observations on the prime factors of $g(n,t)$ that can be drawn from Theorem 7 and Theorem 9. Fixing a prime p and a positive integer α, it is easy to see that all positive integer solutions (i,j) of the two requirements $i - 2j = p^{\alpha}$ and p^{α} divides j are given by the set $\{((2k+1)\, p^{\alpha}, k p^{\alpha}) \,|k = 0, 1, 2, ...\}$. We are interested in knowing the intersection of this set with the triangle $T(n,t)$ of Theorem 9. Note that

$(i,j) \in T(n,t)$ if and only if $n-t \leq i \leq n$ and $j \leq i-(n-t)$. Hence, $((2k+1)p^\alpha, kp^\alpha)$ lies in the intersection if and only if

$$\begin{aligned} n-t &\leq (2k+1)p^\alpha \leq n \\ kp^\alpha &\leq (2k+1)p^\alpha - (n-t) \end{aligned}$$

or equivalently

$$\frac{n-t}{k+1} \leq p^\alpha \leq \frac{n}{2k+1}. \tag{6}$$

The last double inequality suggests the introduction of the following terminology for the purpose of discussing the prime factors of $g(n,t+1)$. For fixed values of n and t we say that a prime p is of type k if there exists a positive integer α such that (6) is satisfied (equivalently, $((2k+1)p^\alpha, kp^\alpha) \in T(n,t)$). Note that a given prime may be of several types. However, for a fixed prime p, a given value of α corresponds to at most one type, and a type uniquely determines a value of α. For the first claim, we get from $t < \left\lfloor \frac{n}{2} \right\rfloor$ that $\frac{n-t}{k+1} > \frac{n}{2k+2}$ and therefore the closed intervals $\left[\frac{n-t}{k+1}, \frac{n}{2k+1}\right]$ are disjoint for different values of k. In order to prove the second claim, observe that the ratio of the two end points of the closed interval $\left[\frac{n-t}{k+1}, \frac{n}{(2k+1)}\right]$ satisfies:

$$\frac{\frac{n}{2k+1}}{\frac{n-t}{k+1}} = \frac{k+1}{2k+1}\frac{1}{1-\frac{t}{n}} < 2\frac{k+1}{2k+1} \leq 2,$$

where we have again used $\frac{t}{n} < \frac{1}{2}$. But this implies that if $p^\alpha \in \left[\frac{n-t}{k+1}, \frac{n}{2k+1}\right]$, then $p^{\alpha-1} < \frac{n-t}{k+1}$ and $p^{\alpha+1} > \frac{n}{2k+1}$, thus proving our claim. We can conclude that, in fact, the number of distinct types a given prime p assumes for a given (n,t) is equal to its multiplicity as a prime factor of $g(n,t+1)$. Another elementary observation is that in order to have a prime factor of type k it is necessary (but obviously not sufficient) that the interval $\left[\frac{n-t}{k+1}, \frac{n}{2k+1}\right]$ is not empty. This gives

$$t \geq \frac{k}{2k+1}n. \tag{7}$$

Since the right hand side of the last inequality is an increasing function of k, we have that for $t < \frac{k}{2k+1}n$ there are no primes of type k or higher.

The results above can be used to prove Granville's Theorem 2. Recall that p and α of the theorem are defined by the requirement that $n - p^\alpha \geq 0$ is minimal. As we will shortly argue, $n - p^\alpha < \frac{n}{2}$ and hence $t = n - p^\alpha$ is a legitimate choice of truncation. Making use of the easy fact that if p is of type k for (n,t'), then it is of type k for (n,t) for any $t \geq t'$, it is sufficient to show the following:

a. p is of type zero for $(n, t = n - p^\alpha)$ but not for $(n, t' < n - p^\alpha)$.

b. For $(n, t = n - p^\alpha)$ there are no other primes of type zero .

c. For $(n, t = n - p^\alpha)$ there are no primes of type one or higher.

Claim (a) is immediate from the definition of a type and the fact that $n - p^\alpha \geq 0$. Claim (b) is immediate from the minimality of $n - p^\alpha$. For Claim (c) recall the discussion which follows (7), according to which there are no primes of type $k \geq 1$ for $(n, t = n - p^\alpha)$ if $n - p^\alpha < \frac{n}{3}$. The inequality $n - p^\alpha < \frac{n}{3}$ follows directly from Nagura's general result on the existence of primes in the interval $\left(x, \frac{6x}{5}\right)$ for $x \geq 25$ (see [6]).

2. Carries and Kummer's theorem

In this section we collect some definitions, notations and properties of carries that will enable us to use Kummer's theorem in order to prove our claims.

Carries are defined relative to a chosen base b representation of the integers involved. Let $b \geq 2$ be an integer. We denote the length l base b representation of a non-negative integer n by $n = (n_{l-1}, n_{l-2}, ..., n_0)_b$, where the digits n_i satisfy $n_i \in \{0, 1, ..., b-1\}$ and $n = \sum_{i=0}^{l-1} n_i b^i$. The positive integer l (called the *length of the representation*) counts the number of digits. Unless otherwise stated, we do not assume that l takes its minimal value, i.e., we allow leading zeros, and we will use the terminology "a legitimate l value" to refer to an arbitrary value l, satisfying $l \geq \lfloor \log_b n \rfloor + 1$. This will enable us to choose a common length when representing several different numbers. When the value of l is immaterial for the discussion, we simply talk about base b representation and leave it unspecified. We now state the definition of the addition carry.

Definition 10 *Let $b \geq 2$ be a positive integer. Let $x \geq 0$, $y \geq 0$ be two integers. Let $x = (x_{l-1}, x_{l-2}, ..., x_0)_b$, $y = (y_{l-1}, y_{l-2}, ..., y_0)_b$ be base b representations of x and y. The ith digit* addition carry *of the pair (x, y) in base b representation is defined to be 1 if*

$$(x_i, x_{i-1}, ..., x_0)_b + (y_i, y_{i-1}, ..., y_0)_b \geq b^{i+1}$$

and 0 otherwise.

Note that the addition carry of the ith digit depends only on the digits in the places $0, ..., i$.

The following lemma, whose proof is left to the interested reader, summarizes some basic properties of the addition carry.

Lemma 11 *Let x, y, b, l be as in Definition 10, and add one leading zero to each of x and y (i.e. $x_l = y_l = 0$). Let c_i denote the addition carry of the ith digit of (x, y), let $n = x + y$ and let $n = (n_l, ..., n_0)_b$ be its length $l + 1$ base b representation. Then:*

1. c_i is determined recursively from c_{i-1}, for all $0 \leq i \leq l$, by:

$$\begin{cases} 1, & \text{if } x_i + y_i + c_{i-1} \geq b \\ 0, & \text{otherwise,} \end{cases}$$

where $c_{-1} = 0$. Moreover, for all $0 \leq i \leq l$ we have:

$$n_i = \begin{cases} x_i + y_i + c_{i-1}, & \text{if } c_i = 0 \\ x_i + y_i + c_{i-1} - b, & \text{if } c_i = 1 \end{cases}. \tag{8}$$

Note that $c_l = 0$ and $n_l = c_{l-1}$.

2. The addition carry of the ith digit of (x, y) is equal to the addition carry of the ith digit of (y, x).

3. For all $0 \leq i \leq l-1$, if $c_i = 0$, then $n_i \geq \max\{x_i, y_i\}$, and if $c_i = 1$, then $n_i \leq \min\{x_i, y_i\}$.

There is an alternative definition of a carry which is associated with the subtraction rather than the addition of two numbers. We have found it more convenient to formulate the proof of the main result in terms of the subtraction carry.

Definition 12 *Let $b \geq 2$ be a positive integer. Let $n \geq 0$, $k \geq 0$ be two integers. Let $n = (n_{l-1}, ..., n_0)_b$ and $k = (k_{l-1}, ..., k_0)_b$ be base b representations of n and k. For all $0 \leq i \leq l-1$, the* subtraction carry *of the ith digit of (n, k) in base b representation is defined to be 1 if there exists $0 \leq s \leq i$ satisfying:*

$$\begin{aligned} &n_s < k_s, \\ &n_j = k_j \quad ; \quad \text{for all } j \text{ such that } s+1 \leq j \leq i, \end{aligned}$$

and 0 otherwise.

Note that if $s = i$, then only $n_s < k_s$ is relevant.

The precise sense in which these two types of carries are equivalent is clarified by the next lemma.

Lemma 13 *Let x, y, b, l be as in Definition 10. For all $0 \leq i \leq l-1$ we have $c_i = c'_i$, where c_i is the addition carry of the ith digit of (x, y) and c'_i is the subtraction carry of the ith digit of $(x + y, y)$. Similarly, if n, k, b, l are as in Definition 12 and $n \geq k \geq 0$, then $c_i = c'_i$ for all $0 \leq i \leq l-1$, where c_i is the addition carry of the ith digit of $(k, n-k)$ and c'_i is the subtraction carry of the ith digit of (n, k).*

Lemma 13 can be proved by induction on l. We omit the details.

Remark 14 We will denote the subtraction carry of the ith digit of (n,k) in a base b representation by $c_i(n,k,b)$. The reader will notice that Definition 12 extends Definition 10, since the subtraction carry is defined even for $n<k$, for which case Lemma 13 does not suggest corresponding x,y values. The proof of our main result makes use of this extension. Henceforth, the term carry will stand for subtraction carry.

Corollary 15 *If $n \geq k \geq 0$, then $c_i(n,k,b) = c_i(n,n-k,b)$.*

Proof. This is immediate from Claim 2 of Lemma 11. □

Definition 16 *Let n,k,b,l be as in Definition 12. The* (total) carry *of (n,k) in the length l base b representation will be denoted $C^{(l)}(n,k,b)$. It is defined to be the sum of the carries of the digits, namely:*

$$C^{(l)}(n,k,b) = \sum_{i=0}^{l-1} c_i(n,k,b).$$

The carry of (n,k) in the base b representation will be denoted $C(n,k,b)$ and is defined to be $C^{(l)}(n,k,b)$ for the unique legitimate value of l such that n_{l-1} or k_{l-1} are non-zero.

Whenever the base b is fixed at the start of the discussion or is clear from the context, we will allow ourselves to omit it, e.g., write $C(n,k)$ instead of $C(n,k,b)$, etc.

Remark 17 Note that if $n \geq k \geq 0$ in the last definition, then $C(n,k,b) = C^{(l)}(n,k,b)$ for all legitimate l values. In other words, leading zeros in n do not affect the carries. This last statement is clearly not true if $n<k$.

Let p be a prime, α a non-negative integer and n an integer. We say that p^α divides n *exactly* (equivalently, p^α is the *exact power* of p dividing n), if p^α divides n but $p^{\alpha+1}$ does not divide n.

Kummer's theorem, stated in terms of the total carry defined above, reads as follows.

Theorem 18 *(Kummer) Let $n \geq k \geq 0$ be any two integers. Let p be any prime number. Suppose that p^α divides the binomial coefficient $\binom{n}{k}$ exactly. Then $\alpha = C(n,k,p)$.*

Example 19 Suppose we want to find the exact power of 2 dividing $\binom{9}{3}$. According to the theorem, this is $C(9,3,2)$. Let us use this example to illustrate both carry Definitions

10 and 12 (which are equivalent in this case). Adding $6 = (110)_2$ and $3 = (011)_2$ in base 2 we get (the two addition carries appear on the top line):

$$\begin{array}{ccccc} 1 & 1 & & & \\ & 1 & 1 & 0 & + \\ & 0 & 1 & 1 & \\ - & - & - & - & - \\ 1 & 0 & 0 & 1 & \end{array}$$

giving $C(9,3,2) = 2$. In order to compute the same quantity as a substraction carry, we use the representations $9 = (1001)_2$ and $3 = (0011)_2$ and find $c_3 = c_0 = 0$ and $c_2 = c_1 = 1$, giving $C(9,3,2) = 2$ as well. Thus, by Kummer's theorem 2^2 divides $\binom{9}{3}$ exactly. Indeed $\binom{9}{3} = \frac{9\cdot 8\cdot 7}{3\cdot 2\cdot 1} = 2^2 \cdot 3 \cdot 7$.

We now state and prove three lemmas about properties of the total carry. These lemmas will form the basis for the proofs of our main results.

Lemma 20 *Using the notation of Definition 12, assume the existence of an index* $0 \leq m \leq l-1$ *satisfying* $n_m \neq k_m$. *Define* n', k', n'', k'' *by:*

$$\begin{aligned} n' &= n_{m-1}b^{m-1} + ... + n_1 b + n_0, \\ k' &= k_{m-1}b^{m-1} + ... + k_1 b + k_0, \\ n &= n'' + n', \\ k &= k'' + k', \end{aligned}$$

where $m = 0$ *implies* $n' = k' = 0$. *Then*

$$C(n,k) = C(n'',k'') + C^{(m)}(n',k'). \tag{9}$$

In particular, if m *is the minimal index satisfying* $n_m \neq k_m$, *and if* $n \geq k$, *then*

$$C(n,k) = C\left(\left\lfloor \frac{n}{b^m} \right\rfloor, \left\lfloor \frac{k}{b^m} \right\rfloor\right). \tag{10}$$

Proof. Consider any $0 \leq i \leq l-1$. By Definition 12, $c_i(n,k)$ is determined by the largest $0 \leq j \leq i$ such that $n_j \neq k_j$. Hence, for $i < m$ we have $c_i(n,k) = c_i(n',k')$. For $i \geq m$, this maximal j value satisfies $j \geq m$, since $n_m \neq k_m$. Hence, in this case, $c_i(n,k) = c_i(n'',k'')$. Equation (9) now follows. Furthermore, if m is the minimal index satisfying $n_m \neq k_m$, then $C^{(m)}(n',k') = 0$. Division by b^m has the effect of shifting the base b digits m places to the right, thus giving (10). □

Lemma 21 *Let* $n > k \geq 0$ *be integers and* $n_0 \neq k_0$ *their least significant digits in base* b. *Then:*

1. $C(n,k+1) \leq C(n,k)$
2. $C(n-1,k) \leq C(n,k)$.

Proof. We use the notation of Definition 12, and prove the lemma by induction on $l \geq 1$.

1. For $l = 1$, we have $n = n_0 > k = k_0$. Hence $C(n,k) = 0$, and since $n_0 \geq k_0 + 1$ we also have $C(n,k+1) = 0$. For a general $l > 1$ we split the discussion into two cases.

a. $n_0 > k_0$ or $n_0 < k_0 < b-1$. In this case $C(n,k) = C(n,k+1)$.

b. $n_0 < k_0 = b-1$. In this case let $m > 0$ be the minimal index satisfying $n_m \neq k_m$ (it exists since $n > k$ and $n_0 < k_0$). Define n', k', n'', k''

$$\begin{aligned} n' &= n_{m-1}b^{m-1} + ... + n_1 b + n_0, \\ k' &= n_{m-1}b^{m-1} + ... + n_1 b + k_0, \\ n &= n' + n'', \\ k &= k' + k''. \end{aligned}$$

Then, by Lemma 20 (9):

$$C(n,k) = C(n'',k'') + C^{(m)}(n',k') = C(n'',k'') + m.$$

Let $0 \leq s \leq m-1$ be the greatest index for which $k_i = b-1$ for all $0 \leq i \leq s$ ($s+1$ is the length of a maximal $b-1$ suffix of k'). If $s < m-1$ we have:

$$\begin{aligned} C(n,k+1) &= C(n'',k'') + C^{(m)}(n',k'+1) \\ &= C(n'',k'') + C^{(m)}(n',k') - (s+1) \\ &= C(n'',k'') + m - (s+1) < C(n'',k'') + m \\ &= C(n,k), \end{aligned}$$

because $c_i(n',k'+1) = 0$ for all $0 \leq i \leq s$, and the $s+1$ digit of $k'+1$ is $n_{s+1}+1$. If $s = m-1$, then $k'+1 = b^m$ and $k+1 = k''+k'+1 = k''+b^m$. As a result, we have (by Lemma 20 (9)):

$$\begin{aligned} C(n,k+1) &= C(n'',k''+b^m) + C^{(m)}(n',0) \\ &= C(n'',k''+b^m). \end{aligned}$$

Now since b^m divides n'' and k'', by Lemma 20 (10) we have:

$$\begin{aligned} C(n'',k'') &= C\left(\frac{n''}{b^m}, \frac{k''}{b^m}\right), \\ C(n'',k''+b^m) &= C\left(\frac{n''}{b^m}, \frac{k''}{b^m}+1\right). \end{aligned}$$

Since $m > 0$, $\frac{n''}{b^m}, \frac{k''}{b^m}$ have less than l digits, and we can apply the induction assumption (by definition of m we have $n_m \neq k_m$) and deduce

$$C\left(\frac{n''}{b^m}, \frac{k''}{b^m}+1\right) \leq C\left(\frac{n''}{b^m}, \frac{k''}{b^m}\right).$$

This proves $C(n,k+1) < C(n,k)$ also for this case.

2. The proof of the second claim can be carried along the lines of the proof of the first claim. We leave out the details. □

Lemma 22 *Let $n > k \geq 0$ be integers and let the notation be as in Definition 12. Let m be the minimal index satisfying $n_m \neq k_m$. Set $x = n_{m-1}b^{m-1} + ... + n_0$ (if $m = 0$, then $x = 0$) and $s_0 = k + b^m - x$. Then:*

1. $C(n,s_0) \leq C(n,k)$.

2. $C(n-b^m,k) \leq C(n,k)$.

3. For all $k+1 \leq s < s_0$ we have $C(n,s) > C(n,k)$. Furthermore, if $x < b^m - 1$, then

$$\min_{k+1 \leq s < s_0} C(n,s) = C(n,k) + r + 1,$$

where $0 \leq r < m$ is defined to be the length of the $b-1$ prefix of x, i.e.,

$$\begin{aligned} &\text{if } n_{m-1} \neq b-1, \text{ then } r = 0, \\ &\text{else } n_{m-1} = ... = n_{m-r} = b-1 \text{ and } n_{m-(r+1)} \neq b-1. \end{aligned}$$

Proof. The first two claims just generalize the claims of Lemma 21 and can be proved by reducing to it. We omit the details. To prove the third claim, fix an arbitrary $k+1 \leq s < s_0$ and set $y = s-k$, $n'' = n-x$, $k'' = k-x$. We have

$$C(n,s) = C(n''+x, k''+x+y)..$$

Observe that $k+1 \leq s < s_0$ is equivalent to $1 \leq y < b^m - x$. In particular, since $x + y < b^m$ we can apply Lemma 20 and get:

$$\begin{aligned} C(n,s) &= C(n'',k'') + C^{(m)}(x, x+y) \\ &= C(n,k) + C^{(m)}(x, x+y). \end{aligned}$$

Moreover, $x + y > x$ implies $C^{(m)}(x, x+y) > 0$, and therefore $C(n,s) > C(n,k)$ for all $k+1 \leq s < s_0$.

In order to prove the quantitative part of the third claim, we will prove the equivalent claim:

$$\min_{1 \leq y < b^m - x} C^{(m)}(x, x+y) = r+1.$$

Set $\overline{y} = b^{m-r-1}$. We have $1 \leq \overline{y} < b^m - x$ and $C^{(m)}(x, x+\overline{y}) = r+1$, since $c_i(x, x+\overline{y}) = 0$ for all $0 \leq i \leq m-r-2$, and $c_i(x, x+\overline{y}) = 1$ for all $m-r-1 \leq i \leq m-1$.

Fix $y \geq 1$ such that $x + y < b^m$. Then, the base b representation of $x + y$ is of length no greater than m. Let $(d_{m-1}, d_{m-2}, ..., d_0)_b$ be the length m base b representation of $x + y$. Let f be the first index from the left for which $d_f \neq n_f$. Since $x + y > x$, we must have $d_f > n_f$. But the first r digits of x from the left (with indices $m-1, ..., m-r$) are maximal (i.e., equal to $b-1$), so $f \leq m - r - 1$ implying $C^{(m)}(x, x+y) \geq r+1$. This proves that $\overline{y}$ attains the minimum. □

3. Proofs of the Main Results

In our proofs we will use the following direct consequence of Kummer's theorem:

Fix an arbitrary prime p. There exists a non-negative integer $\alpha_{n,t,p}$ such that $p^{\alpha_{n,t,p}}$ divides $g(n,t)$ exactly. Then

$$\alpha_{n,t,p} = \min_{t \leq s \leq \left\lfloor \frac{n}{2} \right\rfloor} C(n, s, p). \tag{11}$$

Proof of Theorem 4: Suppose $n = p^\alpha$ with p prime and $\alpha > 0$. Let s be any integer in the range $1 \leq s \leq \left\lfloor \frac{p^\alpha}{2} \right\rfloor$. In base p the number p^α has an $\alpha+1$ length representation $p^\alpha = (1, 0, ..., 0)_p$. Since $1 \leq s \leq \left\lfloor \frac{p^\alpha}{2} \right\rfloor$, it follows that the base p, $\alpha+1$ length representation of s has at least one non-zero digit at position less than $\alpha+1$. Hence $C(p^\alpha, s, p) \geq 1$ for all $1 \leq s \leq \left\lfloor \frac{p^\alpha}{2} \right\rfloor$. From (11) we get $\alpha_{p^\alpha,1,p} \geq 1$. On the other hand, $C(p^\alpha, p^{\alpha-1}, p) = 1$, whence $\alpha_{p^\alpha,1,p} = 1$. Now consider any other prime $q \neq p$. Since q does not divide $\binom{n}{1} = p^\alpha$, we get $\alpha_{p^\alpha,1,q} = 0$.

We have proved that for $n = p^\alpha$ with p prime and α a positive integer, we get $g(n,1) = p$. Now consider n which is not a prime power. Let p be any prime. Let $\alpha \geq 0$ be an integer such that p^α divides n exactly. By assumption $n \neq p^\alpha$, and so $p^\alpha \leq \left\lfloor \frac{n}{2} \right\rfloor$. It is easy to see that $C(n, p^\alpha, p) = 0$, and therefore $\alpha_{n,p^\alpha,p} = 0$. This shows that if n is not a prime power, then $g(n,1)$ has no prime divisor and so $g(n,1) = 1$. □

Proof of Theorem 5: It is clear that $g(n,t)$ divides $g(n,t+1)$, and so it remains to prove that $g(n-1,t)$ divides $g(n,t+1)$. In order to prove the last claim we use Pascal's law.

$$g(n,t+1) = \gcd\left(\binom{n}{t+1}, \binom{n}{t+2}, ..., \binom{n}{\left\lfloor \frac{n}{2} \right\rfloor}\right) =$$

$$\gcd\left(\binom{n-1}{t+1} + \binom{n-1}{t}, \binom{n-1}{t+2} + \binom{n-1}{t+1}, ..., \binom{n-1}{\left\lfloor \frac{n}{2} \right\rfloor} + \binom{n-1}{\left\lfloor \frac{n}{2} \right\rfloor - 1}\right).$$

Clearly $g(n-1,t)$ divides all entries in the last gcd, and so the claim holds. □

Proof of Theorem 7: Fix an arbitrary prime p. There exist non-negative integers $\alpha_{n,t}$ and $\beta_{n,t}$ such that $p^{\alpha_{n,t}}$ divides $g(n,t)$ exactly, and $p^{\beta_{n,t}}$ divides $h(n,t)$ exactly. From basic properties of lcm we have:

$$\beta_{n,t} = \alpha_{n,t+1} - \max(\alpha_{n,t}, \alpha_{n-1,t}),$$

where, by (11) (suppressing the dependence on p):

$$\alpha_{n,t} = \min_{t \le s \le \left\lfloor \frac{n}{2} \right\rfloor} C(n,s).$$

The conditions of Lemma 22 hold with $n = n$, $k = t$ and $b = p$. By the first claim of the lemma we have $C(n,s_0) \le C(n,t)$, where $s_0 = t + p^m - x$, $x = n_{m-1}p^{m-1} + ... + n_0$, and m is the minimal index satisfying $n_m \neq t_m$. Note that $s_0 \ge t+1$. If, in addition, $s_0 \le \left\lfloor \frac{n}{2} \right\rfloor$, then $\alpha_{n,t} = \alpha_{n,t+1}$, and $\beta_{n,t} = 0$.

Now we consider the case $s_0 > \left\lfloor \frac{n}{2} \right\rfloor$. By the third claim of Lemma 22, $C(n,t) < C(n,s)$ for all $t+1 \le s \le \left\lfloor \frac{n}{2} \right\rfloor$, and hence $\alpha_{n,t+1} > \alpha_{n,t}$ and

$$\alpha_{n,t} = C(n,t). \tag{12}$$

In order to get more of the third part of the lemma we analyze the inequality $s_0 > \left\lfloor \frac{n}{2} \right\rfloor$. First note that this is equivalent to $2s_0 > n$. Substituting $s_0 = t + p^m - x$ and $n = n'' + x$, $t = t'' + x$, we get:

$$n'' - 2t'' < 2p^m - x.$$

On the other hand, $t < \left\lfloor \frac{n}{2} \right\rfloor$ gives $2t < n$ and so:

$$x < n'' - 2t'',$$

which together with $x \ge 0$ gives:

$$0 \le n'' - 2t'' < 2p^m. \tag{13}$$

However, p^m divides n'' and t'', so p^m divides $(n'' - 2t'')$. Together with the last inequality this gives:

$$n'' - 2t'' = p^m. \tag{14}$$

We have

$$\alpha_{n,t+1} = \min_{t+1 \le s \le \left\lfloor \frac{n}{2} \right\rfloor} C(n,s) = \min_{t+1 \le s \le n-t-1} C(n,s),$$

where in the second equality we have used Corollary 15. Now, by (14), we have

$$n - t - 1 = n'' - t'' - 1 = t'' + p^m - 1 = s_0 - 1.$$

We therefore get:

$$\alpha_{n,t+1} = \min_{t+1 \le s < s_0} C(n,s),$$

and now we can conclude from the third part of Lemma 22

$$\alpha_{n,t+1} = C(n,t) + r + 1, \tag{15}$$

where r is the length of the largest prefix of x having all digits equal to $p-1$. Note that in order to use this part of the lemma we must check that $x < p^m - 1$. Indeed, $x = p^m - 1$ implies $s_0 = t + 1$. Since we assume $t < \left\lfloor \frac{n}{2} \right\rfloor$, we get $s_0 \leq \left\lfloor \frac{n}{2} \right\rfloor$ contradicting $s_0 > \left\lfloor \frac{n}{2} \right\rfloor$.

Now consider

$$\begin{aligned}\alpha_{n-1,t} &= \min_{t \leq s \leq \left\lfloor \frac{n-1}{2} \right\rfloor} C(n-1,s) = \\ &= \min_{t \leq s \leq (n-1)-t} C(n-1,s) = \\ &= \min_{t \leq s < s_0} C(n-1,s).\end{aligned}$$

Let $n-1 = (\overline{n}_{l-1}, ..., \overline{n}_0)_p$ and $t-1 = \left(\overline{t}_{l-1}, ..., \overline{t}_0\right)_p$, where $\overline{n}_{l-1}$ might be zero. Observe that m is also the minimal index for which $\overline{n}_m \neq \overline{t}_m$. Let $y = \overline{n}_{m-1}p^{m-1} + ... + \overline{n}_0$. We have two possibilities:

1. $x > 0$. Then $n-1 = n'' + y$, $t-1 = t'' + y$, and $y = x-1$. Note that

$$\begin{aligned}s_0 &= t + p^m - x = t - 1 + p^m - (x-1) = \\ &= t - 1 + p^m - y.\end{aligned}$$

We have $s_0 > \left\lfloor \frac{n-1}{2} \right\rfloor$, since $s_0 > \left\lfloor \frac{n}{2} \right\rfloor$. By the third part of Lemma 22, substituting $n-1$ for n, $t-1$ for k, and y for x (the conditions in Notation 6 assure $n-1 > t-1 \geq 0$), we get $C(n-1, t-1) < C(n-1, s)$ for all $t-1+1 = t \leq s \leq \left\lfloor \frac{n-1}{2} \right\rfloor$. Moreover:

$$\alpha_{n-1,t-1+1} = \alpha_{n-1,t} = C(n-1, t-1) + r' + 1,$$

where r' is the length of the largest prefix of y having all digits equal to $p-1$. Finally, $C(n-1, t-1) = C(n,t)$ since both are equal to $C(n'', t'')$ by Lemma 20. Hence we get:

$$\alpha_{n-1,t} = C(n,t) + r' + 1. \tag{16}$$

Clearly $r' = r$, unless all digits of x to the right of the $p-1$ prefix are zero. Let us consider this last possibility, namely, that $n_i = 0$ for all $0 \leq i < m - r$. If $r = 0$ the $p-1$ prefix is empty, implying $x = 0$, and thus contradicting our current assumption $x > 0$. Otherwise, $r > 0$, and we get $r' = r - 1$.

Putting together all the conclusions derived from the assumption $x > 0$, we either have $r' = r$ or $r' = r - 1$. If $r' = r$, then $\alpha_{n,t+1} = \alpha_{n-1,t}$, and $\beta_{n,t} = 0$. If $r' = r - 1$, then $\alpha_{n,t+1} = \alpha_{n-1,t} + 1$, and $\beta_{n,t} = 1$.

2. $x = 0$. In this case $C(n-1, t) = C(n-1, s)$ for all $t \leq s \leq \left\lfloor \frac{n-1}{2} \right\rfloor$. In order to see this, observe that $s \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ and $s_0 > \left\lfloor \frac{n}{2} \right\rfloor$ give $s < s_0 = t + p^m$, and therefore $0 \leq s - t < p^m$. Write $s = s'' + s'$ with s' composed of the m rightmost base p digits of s (in particular $0 \leq s' < p^m$). Since $x = 0$, we have $t = t''$, and hence $s - t = s'' - t'' + s'$.

The inequality $0 \leq s'' - t'' + s' < p^m$ is consistent with $0 \leq s' < p^m$ and $s'', t'' \geq p^m$ if and only if $s'' = t''$. In other words, s and t may differ only in their m rightmost digits. But $x = 0$ also implies that the m rightmost digits of $n-1$ are $p-1$, so the m rightmost digits of s and t do not contribute to $C(n-1, s)$ and $C(n-1, t)$. Therefore, in this case, $\alpha_{n-1,t} = C(n-1, t)$. Moreover, writing $n - 1 = n'' - p^m + p^m - 1$, we get, for the same reason, $C(n-1, t) = C(n'' - p^m, t)$. Using the second claim of Lemma 22, we get $C(n'' - p^m, t) \leq C(n'', t) = C(n, t)$. Using (15) with $r = 0$ (since $x = 0$), we get $\alpha_{n,t+1} = \alpha_{n,t} + 1$ and $\beta_{n,t} = 1$.

Let us summarize what has been proved so far. We have shown that $\beta_{n,t}$ is either 0 or 1 and, furthermore, that $\beta_{n,t} = 1$ if and only if the following condition holds: $s_0 > \left\lfloor \frac{n}{2} \right\rfloor$ and, in addition, x has an m length base p representation of the form

$$x = (p-1, p-1, ..., p-1, 0, ..., 0)_p, \tag{17}$$

where the length r of the $p-1$ prefix satisfies $0 \leq r < m$.

Now we prove that $\beta_{n,t} = 1$ implies $n - 2t = p^i$ for some $i > 0$, where p^i divides t. Equation (17) gives:

$$n - 2t = n'' - 2t'' - x = p^m - x = p^{m-r}.$$

Since p^{m-r} divides x (by (17)) and t'', it divides t as well.

Finally, let us verify that the conditions stated in the theorem are also sufficient. We will show that if p^i divides t, where p is a prime and i is a positive integer, then $h(2t + p^i, t) = p$, or equivalently that $\beta_{2t+p^i,t} = 1$. Note that by what has been proved so far, this is equivalent to $\beta_{2t+p^i,t} > 0$. We have:

$$\begin{aligned}
\beta_{2t+p^i,t} &= \alpha_{2t+p^i,t+1} - \max\left(\alpha_{2t+p^i,t}, \alpha_{2t+p^i-1,t}\right) \ ; \\
\alpha_{2t+p^i,t+1} &= \min_{1 \leq \Delta \leq \left\lfloor \frac{p^i}{2} \right\rfloor} C\left(2t + p^i, t + \Delta\right) \ ; \\
\alpha_{2t+p^i,t} &= \min_{0 \leq \Delta \leq \left\lfloor \frac{p^i}{2} \right\rfloor} C\left(2t + p^i, t + \Delta\right) \ ; \\
\alpha_{2t+p^i-1,t} &= \min_{0 \leq \Delta \leq \left\lfloor \frac{p^i-1}{2} \right\rfloor} C\left(2t + p^i - 1, t + \Delta\right).
\end{aligned} \tag{18}$$

Let ld_Δ denote the index of the leading digit (the highest non-zero digit) of Δ in base p. If $1 \leq \Delta \leq \left\lfloor \frac{p^i}{2} \right\rfloor$, then $ld_\Delta < i$. On the other hand, the index of the least significant non-zero digit of $2t + p^i$ in base p is at least i. ¿From here we can conclude

$$\alpha_{2t+p^i,t} = C\left(2t + p^i, t\right) < \alpha_{2t+p^i,t+1}. \tag{19}$$

It remains to prove $\alpha_{2t+p^i-1,t} < \alpha_{2t+p^i,t+1}$ as well.

Each of the first i rightmost digits of $2t + p^i - 1$ in base p is equal to $p-1$. This gives

$$C\left(2t + p^i - 1, t + \Delta\right) = C\left(2t + p^i - 1, t\right)$$

for all $0 \leq \Delta \leq \left\lfloor \frac{p^i-1}{2} \right\rfloor$. Hence,

$$\alpha_{2t+p^i-1,t} = C\left(2t+p^i-1,t\right) = C\left(2t,t\right). \tag{20}$$

Now we distinguish two cases:

a. p^{i+1} divides t. In this case we also have $C\left(2t+p^i,t\right) = C\left(2t,t\right)$. Using (20) and (19) we get $\alpha_{2t+p^i-1,t} < \alpha_{2t+p^i,t+1}$.

b. p^{i+1} does not divide t. Let $2t+p^i = \left(n_{l-1},...,n_0\right)_p$ and $t = \left(t_{l-1},...,t_0\right)_p$. Let m be the first index on the right such that $n_m \neq t_m$. Note that $m \geq i$. If $m = i$, we get from the second claim of Lemma 22 that $C\left(2t,t\right) \leq C\left(2t+p^i,t\right)$. This implies, as in case (a), $\alpha_{2t+p^i-1,t} < \alpha_{2t+p^i,t+1}$. If $m > i$, we claim that necessarily $n_{m-1} = ... = n_i = p-1$. In order to prove this last claim, start from $t_i = n_i$. This implies $2t_i + 1 = t_i \left(\mathrm{mod}\, p\right)$, which implies $t_i = n_i = p-1$. Now complete the argument by induction, noting that the jth digit, where $i \leq j < m$, of $2t+p^i$ is $\left(2t_j+1\right) \mathrm{mod}\, p$. For $i < j < m$ this fact follows from the induction assumption. Set $x = t_{m-1}p^{m-1} + ... + t_0$ and $2t+p^i = n'' + x$, $t = t'' + x$. Note that the previous claim implies $2t = n'' + y$, where $y = x - p^i$ differs from x only in the ith digit (being $p-2$ in y and $p-1$ in x). Hence, by the third part of Lemma 22 we get:

$$C\left(2t,t\right) = C\left(n'',t''\right) + m - i,$$
$$C\left(2t+p^i,t+\Delta\right) = C\left(n'',t''\right) + m - ld_\Delta;\ \forall 1 \leq \Delta \leq \left\lfloor \frac{p^i}{2} \right\rfloor.$$

Again, since $ld_\Delta < i$ we get ((18) and (20)) $\alpha_{2t+p^i-1,t} < \alpha_{2t+p^i,t+1}$, as desired. □

The following lemma is needed for the proof of Theorem 9. The reader may consult Figure 1 in order to get an intuitive understanding of its claim. It says that a prime entry of the h-triangle which lies on the segment $D-E$ does not appear on the segment $F-G$ and vice versa.

Lemma 23 *Fix a pair of integers (n,t) such that $n \geq 2$ and $0 \leq t < \left\lfloor \frac{n}{2} \right\rfloor$. Then there do not exist a prime p, positive integers α,β and integers c,$\widetilde{c}$ satisfying simultaneously:*

$$h\left((n-t)+c,c\right) = h\left(n,\widetilde{c}\right) = p,$$
$$0 \leq c,\widetilde{c} \leq t-1\ .$$

Proof. By Theorem 7 and (5), the above set of requirements is satisfied if and only if there exist two positive integers α,β and $p,c,\widetilde{c}$ as above such that:

$$\begin{aligned} (n-t)-c = p^\alpha\ ;&\ \ p^\alpha \text{ divides } c \\ n-2\widetilde{c} = p^\beta\ ;&\ \ p^\beta \text{ divides } \widetilde{c} \\ 0 \leq c,\widetilde{c} \leq t-1.& \end{aligned} \tag{21}$$

First observe that if there exist $\alpha, \beta, p, c, \widetilde{c}$, satisfying the system of conditions (21), then $n, t, c, \widetilde{c}$ are all divisible by p. We will use this fact repeatedly. We start by showing that the system (21) has no solutions with $\alpha = 1$ or with $\beta = 1$.

Case $\alpha = 1$: Since n, t, c are all divisible by p, there exist n_0, t_0, c_0 such that $n = n_0 p$, $t = t_0 p$ and $c = c_0 p$. The condition $(n - t) - c = p$ gives:

$$n_0 - t_0 = c_0 + 1.$$

The inequality $c \leq t - 1$ gives $c_0 \leq t_0 - \frac{1}{p}$, implying $c_0 \leq t_0 - 1$. Using this in the last equation gives $t_0 \geq \frac{n_0}{2}$, contradicting $t < \left\lfloor \frac{n}{2} \right\rfloor$.

Case $\beta = 1$: Since $n, t, \widetilde{c}$ are all divisible by p, there exist $n_0, t_0, \widetilde{c}_0$ such that $n = n_0 p$, $t = t_0 p$, and $\widetilde{c} = \widetilde{c}_0 p$. Now, $n - 2\widetilde{c} = p^\beta$ gives $n_0 = 2\widetilde{c}_0 + 1$. The inequality $\widetilde{c} \leq t - 1$ gives $\widetilde{c}_0 \leq t_0 - 1$. Together with $n_0 = 2\widetilde{c}_0 + 1$, this implies $n_0 \leq 2t_0 - 1$, giving $t_0 \geq \frac{n_0+1}{2}$, contradicting $t < \left\lfloor \frac{n}{2} \right\rfloor$.

We now conclude the proof of the lemma by induction on $n \geq 2$. For $n = 2$ the condition $0 \leq t < \left\lfloor \frac{n}{2} \right\rfloor$ implies $t = 0$. Hence, there are no c,$\widetilde{c}$ satisfying the required inequalities. For a general $n > 2$, assume by contradiction that system (21) has a solution. We have proved above that such a solution must have $\alpha \geq 2$ and $\beta \geq 2$. Set $n' = \frac{n}{p}$, $t' = \frac{t}{p}$, $c' = \frac{c}{p}$, $\widetilde{c}' = \frac{\widetilde{c}}{p}$. These four integers satisfy:

$$\begin{gathered}(n' - t') - c' = p^{\alpha-1} \ ; \ \ p^{\alpha-1} \text{ divides } c' \\ n' - 2\widetilde{c}' = p^{\beta-1} \ ; \ \ p^{\beta-1} \text{ divides } \widetilde{c}' \\ 0 \leq c', \widetilde{c}' \leq t' - 1,\end{gathered}$$

thus contradicting the induction assumption. □

Proof of Theorem 9: From the defining equation of $h(n, t)$ (Notation 6) we obtain, for all $0 \leq t < \left\lfloor \frac{n}{2} \right\rfloor$ and $n \geq 2$:

$$g(n, t+1) = \operatorname{lcm}\left(g(n-1, t), g(n, t)\right) \cdot h(n, t). \tag{22}$$

Now we can proceed by induction on t. For $t = 0$ we get the result from (2), (5) and (3). For a general $t > 0$, we get from (22) that the prime factors of $g(n, t+1)$ are $h(n, t)$ (if it happens to be a prime) and the prime factors of $\operatorname{lcm}\left(g(n-1, t), g(n, t)\right)$. By the induction assumption we have (see Figure 1) :

$$\begin{aligned} g(n-1, t) &= \prod_{(i,j) \in T(n-1, t-1)} h(i, j) \\ &= \prod_{(i,j) \in T(n-1, t-2)} h(i, j) \cdot \prod_{j=0}^{t-1} h(n - t + j, j) \end{aligned}$$

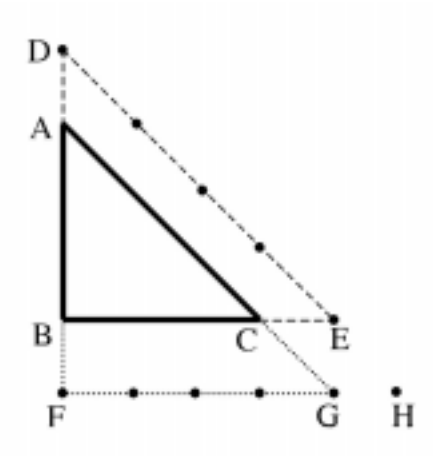

Figure 1: Decomposition of T(n,t) according to Equations (23) and (24).

and

$$g(n,t) = \prod_{(i,j)\in T(n,t-1)} h(i,j) = \prod_{(i,j)\in T(n-1,t-2)} h(i,j) \cdot \prod_{j=0}^{t-1} h(n,j).$$

A standard property of the least common multiple, $\operatorname{lcm}(ab,ac) = a \operatorname{lcm}(b,c)$, where a,b,c are any three positive integers, gives:

$$\begin{aligned} &\operatorname{lcm}(g(n-1,t), g(n,t)) = \\ &= \prod_{(i,j)\in T(n-1,t-2)} h(i,j) \cdot \operatorname{lcm}\left(\prod_{j=0}^{t-1} h(n-t+j,j), \prod_{j=0}^{t-1} h(n,j) \right). \end{aligned} \tag{23}$$

However, by Lemma 23 the two arguments of the lcm on the right hand side of (23) are coprime, and so we get

$$\operatorname{lcm}(g(n-1,t), g(n,t)) = \prod_{(i,j)\in T(n,t-1)\cup T(n-1,t-1)} h(i,j),$$

and we complete the argument by observing that

$$T(n,t) = T(n,t-1) \cup T(n-1,t-1) \cup \{(n,t)\}. \tag{24}$$

□

The geometrical picture behind the last equation is illustrated in Figure 1:

$T(n-1,t-2) = \Delta ABC$;
$T(n-1,t-1) = \Delta DBE$;
$T(n,t-1) = \Delta AFG$; and
$H = (n,t)$.

Acknowledgements: *We would like to express our gratitude to Andrew Granville for his invaluable and encouraging remarks. We also wish to thank the referee for many useful suggestions.*

References

[1] R. C. Baker, G. Harman and J. Pintz, *The difference between consecutive primes, II*, Proc. London. Math. Soc. (3) 83 (2001), 532-562.

[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1996, Berlin, Heidelberg, New-York.

[3] A. Granville, *Arithmetic properties of Binomial Coefficients*, at http://www.dms.umontreal.ca/~andrew/Binomial/.

[4] D. Knuth, *The Art of Computer Programming*, Volume 2, Third Edition, Addison-Wesley, 1997.

[5] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. **44** (1852), 93-146.

[6] C. Soulé, *Secant varieties and successive minima*, arXiv: math.AG/0110254 v1, 23 Oct 2001.