Contemporary Mathematics
http://ojs.wiserpub.com/index.php/CM/

Research Article

The Greatest Common Divisor of Sets of Binomial Coefficients with Restrictions

Chan-Liang Chung[1*], Tse-Chung Yang[2], Kanglun Zhou[3]

[1] School of Mathematics and Statistics, Fuzhou University, Fuzhou 350108, China
[2] Department of Financial Engineering and Actuarial Mathematics, Soochow University, Taipei 100, Taiwan
[3] Department of Mathematics, Yang-En University, Quanzhou 362014, China
E-mail: andrechung@fzu.edu.cn

Received: 23 May 2024; **Revised:** 12 August 2024; **Accepted:** 15 August 2024

Abstract: Ram (1909) proved an elegant result for the greatest common divisor of a set of binomial coefficients, and many researchers have proved similar results along these lines. In this paper, we will turn to the results of the greatest common divisor of sets of binomial coefficients with restrictions. Specifically, we give the answer to $\gcd A_2(n)$ for several cases depending on the value of $s = \sigma_p(n)$ where $p \mid n-1$. (Notations will be introduced below.) We raise some open questions and conjectures for the interested readers to pursuit.

***Keywords*:** binomial coefficient, greatest common divisor, Kummer's theorem, p-adic method

MSC: 11B75, 11A07, 05A10

1. Introduction

In the literature, many mathematicians have studied the divisibility of binomial coefficients. A nice survey and a systematic presentation of this subject were given by Singmaster [1] and Granville [2]. To provide background and motivation, we introduce some common terminology and useful results.

For a positive integer n and a prime number p, we denote the largest integer e, so that n is divisible by p^e, by $\nu_p(n)$. Thus, n can be written as $n = p^e \cdot u$, where u is an integer and $p \nmid u$. Any positive integer n has a unique base-p digit representation

$$n = \sum_{i=0}^{t} c_i p^i = (c_t, c_{t-1}, \ldots, c_0)_p,$$

with minimal $t \geq 0$, $c_t \geq 1$, and $0 \leq c_i \leq p-1$ for all i with $0 \leq i \leq t$. A classical result, the so-called Legendre's formula, was given below

DOI: https://doi.org/10.37256/cm.6120255017

$$\nu_p(n!) = \frac{n - \sigma_p(n)}{p-1},$$

where $\sigma_p(n)$ is denoted by the sum of the base-p digit of n. Another classical result developed by Kummer [3] showed that the power of prime p which divides the binomial coefficient $\binom{n}{k}$ was given by the number of carries when adding k and $n-k$ in the base-p digit representation.

Kummer's theorem For any prime number p, we have

$$\nu_p\left(\binom{n}{k}\right) = \text{the number of carries when adding } k \text{ and } n-k$$

$$\text{in base-}p \text{ digit representation,}$$

where $0 \leq k \leq n$.

In other words, Kummer's theorem said that "$\nu_p\left(\binom{n}{k}\right)$ equals to the number of borrows in base-p subtraction $n-k$".

For any finite subset S of positive integers, we denote the greatest common divisor of all elements of S by $\gcd(S)$, or simply by $\gcd S$. In 1909, Ram proved an elegant theorem on the greatest common divisor among binomial coefficients.

Theorem 1 (Ram [4], 1909) For any integer $n \geq 2$, let S be the set of binomial coefficients

$$S = \left\{ \binom{n}{k} : k = 1, 2, \ldots, n-1 \right\}.$$

Then we have $\gcd S = p$ if $n = p^m$ for some prime p and for some integer $m \geq 1$; and $\gcd S = 1$ for otherwise.

Due to the elegance of Ram's theorem, many researchers prove analogue results along this line. Authors in [5] showed that for any positive integer n, the following holds

$$\gcd\left(\left\{\binom{2n}{2k-1} : 1 \leq k \leq n\right\}\right) = 2^{1+\nu_2(n)}.$$

In [6] Albree generalized the above result by showing that

$$\gcd\left(\left\{\binom{n}{k} : 1 \leq k \leq n, \gcd(k, p) = 1\right\}\right) = p^{\nu_p(n)}, \tag{1}$$

where p is any prime number. This is equivalent to

$$\gcd\left(\left\{\binom{pn}{k} : 1 \leq k \leq pn, p \nmid k\right\}\right) = p^{1+\nu_p(n)}.$$

Another generalization of Ram's result is obtained by [7]. Indeed, in [7] Joris et al. determined

$$d(n; r, s) = \gcd\left(\left\{\binom{n}{k} : r \le k \le s\right\}\right),$$

for any $r \le s \le n$. However, the explicit formula of $d(n; r, s)$ is too complex to illustrate here.

In [8] Hong extended of Albree's result (1). For any positive integers m and n, Hong showed

$$\gcd\left(\left\{\binom{mn}{k} : 1 \le k \le mn, \gcd(k, n) = 1\right\}\right) = n \prod_{p \mid \gcd(m, n)} p^{v_p(m)}. \tag{2}$$

If n or k is required to be a multiple of a positive integer, the situation becomes more complex. The author in [9] proved a tidy generalization of Ram's theorem.

Theorem 2 (McTague [9], 2017) For any integers $n > q > 0$, and for any prime p congruent to 1 modulo q, we have

$$v_p\left[\gcd\left(\left\{\binom{n}{qk} : 1 \le k \le \lfloor n/q \rfloor\right\}\right)\right] = 1,$$

if $\sigma_p(n) \le q$; and the value is equal to 0 for otherwise.

For any positive integer d and any integer $n \ge 2$, consider the set

$$A_d(n) = \left\{\binom{n}{k} : 1 \le k \le n-1,\ \gcd(n, k) = d\right\}.$$

In [8] Hong proved that $\gcd A_1(n) = n$ for all positive integer $n \ge 2$ (the case when $m = 1$ in (2)). In the same paper, Hong proposed a problem which asked a general answer for $\gcd A_d(n)$ when $d > 1$.

For each positive integer $n \ge 2$, the number $b(n)$ is the smallest nonnegative integer such that the set of the binomial coefficients $\binom{n}{k}$, where k is an integer with $b(n) < k < n - b(n)$, has a nontrivial divisor. The existence and the characterization of $b(n)$ can be found in [10]. In fact, the number $b(n)$ is the smallest integer of the form $n - p^e$, where p^e is a prime power less or equal to n. That is, $n = p^e + b(n)$. For examples, $b(22) = 3$ (since $22 = 19 + 3$), and $b(33) = 1$ ($33 = 2^5 + 1$). Let $B_d(n) = \left\{\binom{n}{k} : b(n) < k < n - b(n),\ \gcd(n, k) = d\right\}$.

In a recent paper [11], using methods from both elementary number theory and the p-adic valuation, Xiao et al. proved the complementary result (see Corollary 1.1 in [11]) to Ram's theorem.

Theorem 3 (Xiao et al. [11], 2022) For any integer $n \ge 2$, write $b(n) = n - p^e$. We have

$$\gcd\left\{\binom{n}{k} : b(n) < k < n - b(n)\right\} = p.$$

It is obvious that $\gcd B_1(n) = n$ for all positive integers $n \ge 2$ with $b(n) = 0$. However, the value of $\gcd B_1(n)$ varies, and we have no idea about the exact value.

In this paper, we study the greatest common divisor of sets $A_d(n)$ and $B_d(n)$ when $d = 2$ and answer partially to a problem proposed by [8]. First of all, we can reduce the question about $A_2(n)$ to the case when each component of the base-p representation of n is 0 or 1, where p is a prime divisor of $n - 1$. After that, this case can be divided into three

subcases according to the value of $\sigma_p(n)$. More precisely, the subcases will goes in $\sigma_p(n)=2$, $\sigma_p(n)=4$ and $\sigma_p(n)\geq 6$. In the first case, $\sigma_p(n)=2$, we can determine the exact value of the greatest common divisor of the set $A_2(n)$, namely,

$$\gcd A_2(n)=\frac{n}{2}\cdot p.$$

For the second and third cases, we prove the following main results.

Theorem 4 For $n=p^{t_1}+p^{t_2}+p^{t_3}+1$ $(t_1>t_2>t_3>0)$, let $a_m=v_2(t_m)$, and write $t_m=2^{a_m}u_m$ with odd integers u_m for $m=1,2,3$. Then we have $\nu_p(\gcd A_2(n))=1$ if and only if $a_i=a_j<a_k$ and $a_k=a_i+v_2(u_i-u_j)$ for $\{i,j,k\}=\{1,2,3\}$; and $\nu_p(\gcd A_2(n))=0$ for otherwise.

Theorem 5 For a positive integer n and an odd prime number p, we let

$$n=p^{s-1}+p^{s-2}+\cdots+p+1,$$

where s is an even number, and have $\nu_p(\gcd A_2(n))=0$ if s is not a power of 2. Moreover, for $s=2^b$, we have $\nu_p(\gcd A_2(n))=1$ if $b=2$, or $b=3$ when $p\equiv 1 \pmod 4$; and $\nu_p(\gcd A_2(n))=0$ for otherwise.

This paper is organized as follows. In Section 2, we present some results for $\gcd A_2(n)$ and answer partially to a problem of Hong in [8]. In Section 3, we briefly discuss the value of $\gcd B_d(n)$ for $d=1,2$ and summarize our results. We also raise some open questions and conjectures, and hope that interested readers will continue to explore them.

2. Results for $\gcd A_2(n)$

In what follows, we should use the fact that is not specifically mentioned

$$\nu_p(\gcd S)=\min_{n\in S}\nu_p(n),$$

for any finite subset S of positive integers. Recall that

$$A_d(n)=\left\{\binom{n}{k}: 1\leq k\leq n-1,\ \gcd(n,k)=d\right\}.$$

We begin this section with a simple result when $d=2$.

Proposition 1 For any even integer n with $n-1=p^t$ $(t>0)$, an odd prime power, we have

$$\gcd A_2(n)=(n/2)\cdot p.$$

Proof. Note that both n and k are even, say $n=2t$, $k=2k'$ with two coprime positive integers n' and k'. In light of

$$2k'\binom{n}{k}=2n'\binom{n-1}{k-1},$$

and $\gcd(n', k') = 1$, we obtain that

$$n' = \frac{n}{2} \;\Big|\; \binom{n}{k}, \text{ for each even integer } k \text{ with } 1 \le k \le n-1. \tag{3}$$

Assume that $n-1 = p^t$ for some integer $t > 0$ and odd prime p. We claim that $\gcd A_2(n) = n'p$. Since

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} = \binom{p^t}{k} + \binom{p^t}{k-1} \equiv 0 \pmod{p},$$

and together with (3) we have

$$n'p \;\Big|\; \binom{n}{k}, \text{ for all even } k \text{ with } 1 \le k \le n-1.$$

This implies that $(n/2) \cdot p \mid \gcd A_2(n)$.
On the other hand,

$$\gcd A_2(n) \;\Big|\; \binom{n}{2} = \frac{n}{2} \cdot (n-1) = n'p^t.$$

Therefore, we may assume that $\gcd A_2(n) = n'p^j$ for some j with $0 < j \le t$. If $t = 1$, then $j = 1$ and the proof is done. Suppose $t \ge 2$. Then we have $p^t + 1 - 2p^{t-1} = (p-2)p^{t-1} + 1 > 0$, and the considered binomial coefficient

$$\binom{p^t+1}{2p^{t-1}} \in A_2(n).$$

By Kummer's theorem, we immediately get

$$p \;\Big|\; \binom{p^t+1}{2p^{t-1}} \text{ but } p^2 \nmid \binom{p^t+1}{2p^{t-1}}.$$

That is,

$$\nu_p\left(\binom{p^t+1}{2p^{t-1}}\right) = 1$$

which implies $j = 1$ and our proof completes. □

Remark 1 By the similar argument in the proof of Proposition 1, it follows that

$$\frac{n}{d} \;\Big|\; \binom{n}{k} \text{ for all } k \text{ which is a multiplier of } d \text{ with } 1 \le k \le n-1,$$

and hence

$$\frac{n}{d} \;\Big|\; \gcd A_d(n).$$

Since $\frac{n(n-1)}{2} = \binom{n}{2} \in A_2(n)$ and $\frac{n}{2} \;\Big|\; \gcd A_2(n)$, in order to determine the greatest common divisor of the set $A_2(n)$, we need to consider the values $\nu_p\left(\binom{n}{k}\right)$ for those odd primes p such that $p \mid (n-1)$. For each prime p with $p \mid (n-1)$, consider the base-p representation

$$n = \sum_{i=0}^{t} c_i p^i = (c_t, c_{t-1}, \ldots, c_0)_p.$$

We have $c_0 = 1, \text{ for } p \mid (n-1)$. Together with $p \mid (n-1)$, we have $c_0 = 1$. That is,

$$n = c_t p^t + c_{t-1} p^{t-1} + \cdots + c_1 p + 1,$$

with $0 \le c_i \le p-1$, and $c_t \ge 1$. If there exits some j so that $c_j \ge 2$, we may set $k = 2p^j$ which is even and $\gcd(n, k) = 2$. Hence by Kummer's theorem,

$$\nu_p\left(\binom{n}{k}\right) = 0,$$

which implies that $\nu_p(\gcd A_2(n)) = 0$. We summarize the above discussion as the the following.

Proposition 2 Given an even integer n. For each prime divisor p of $n-1, \text{ consider the base-}p$ representation

$$n = \sum_{i=0}^{t} c_i p^i = (c_t, c_{t-1}, \ldots, c_0)_p.$$

If there exists $c_j \ge 2$ for some $j, \text{ then we have } \nu_p(\gcd A_2(n)) = 0$.

Hence, we can restrict ourselves to the remaining case when $n = c_t p^t + c_{t-1} p^{t-1} + \cdots + c_1 p + 1$ with $c_j \in \{0, 1\}$ for all j between 1 and $t, \text{ where } p$ is a prime divisor of $n-1$. It follows that $c_t = 1$ and let $s := \sigma_p(n) = 2 + \sum_{i=1}^{t-1} c_i \ge 2$ which is an even integer greater than 2 (since $2 \mid n$). Now, we divide it into three subcases **(i)** $s = 2$, **(ii)** $s = 4$, and **(iii)** $s > 4$.

(i) If $s = 2$, $n = (1, 0, \ldots, 0, 1)_p = p^t + 1$ in this case. That is, $n - 1 = p^t$. By the previous Proposition 1, we have

$$\gcd A_2(n) = (n/2) \cdot p.$$

(ii) Assume that $s = 4$ and $n = p^t + p^j + p^i + 1$ $(t > j > i > 0)$. We define the reverse symmetry of n by $\bar{n}$

$$\bar{n} = p^t + p^{t-i} + p^{t-j} + 1.$$

The following results are useful for us to know $\gcd A_2(n)$ when $n = p^t + p^j + p^i + 1$ $(t > j > i > 0)$.

Lemma 1 For any positive integers a, m, and n, let $d = \gcd(m, n)$ and $A = a^d$. Then we have

$$\gcd(a^m + 1, a^n + 1) = \begin{cases} a^{\gcd(m,n)} + 1 = A + 1 & , \text{if } 2 \mid \frac{m+n}{d}, \\ 2 & , \text{if } 2 \nmid \frac{m+n}{d}. \end{cases}$$

Proof. Assume $m = dm'$ and $n = dn'$ for some coprime positive integers m' and n'. Let $D = \gcd(a^m + 1, a^n + 1) = \gcd(A^{m'} + 1, A^{n'} + 1)$. Without loss of generality, we may assume m' is an odd integer. Since $A^{m'} \equiv -1 \equiv A^{n'} \pmod{D}$, we have $A^{2m'} \equiv A^{2n'} \equiv 1 \pmod{D}$. The order, $o(A^2)$, of A^2 in $(\mathbb{Z}/D\mathbb{Z})^\times$ divides both m' and n' which implies $o(A^2) = 1$ since m' and n' are coprime. That is, $A^2 \equiv 1 \pmod{D}$.

Let $m' = 1 + 2j$. Then we have $A^{m'} + 1 = A \cdot (A^2)^j + 1 \equiv A + 1 \pmod{D}$ and $D = \gcd(A^{m'} + 1, D) = \gcd(A + 1, D) = \gcd(A + 1, D \pmod{A+1})$. Note that

$$D \pmod{A+1} = \gcd(A^{m'} + 1, A^{n'} + 1) \pmod{A+1} = \gcd(0, (-1)^{n'} + 1) = (-1)^{n'} + 1.$$

Therefore, we have

$$\begin{aligned} D &= \gcd(A + 1, D \pmod{A+1}) \\ &= \gcd(A + 1, (-1)^{n'} + 1) \\ &= \begin{cases} A + 1, & \text{if } 2 \nmid n'; \\ 2, & \text{if } 2 \mid n', \end{cases} \\ &= \begin{cases} A + 1, & \text{if } 2 \mid (m' + n'); \\ 2, & \text{if } 2 \nmid (m' + n'), \end{cases} \\ &= \begin{cases} A + 1, & \text{if } 2 \mid \frac{m+n}{d}; \\ 2, & \text{if } 2 \nmid \frac{m+n}{d}. \end{cases} \end{aligned}$$

□

In our cases, a weaker form of Lemma 1 might be more useful.

Corollary 1 For positive integers m, n and an odd integer $a > 1$, then we have

$$\gcd(a^m + 1, a^n + 1) = \begin{cases} > 2, & \text{if } \nu_2(m) = \nu_2(n); \\ 2, & \text{if } \nu_2(m) \neq \nu_2(n). \end{cases} \tag{4}$$

For any positive integers m and n, we can define the relation $\sim_a$ by $m \sim_a n$ if $\gcd(a^m+1, a^n+1) > 2$ and it is easy to see that $\sim_a$ is an equivalent relation.

The following proposition tells us the relation between $\gcd A_2(n)$ and $\gcd A_2(\bar{n})$.

Proposition 3 If $\sigma_p(n) = 4$ for some odd prime p with $p \mid (n-1)$, we have $p \mid \gcd A_2(n)$ if and only if $p \mid \gcd A_2(\bar{n})$.

Proof. Assume that $n = p^t + p^j + p^i + 1$ $(t > j > i > 0)$. According to Kummer's theorem and the symmetric property of the binomials coefficients $\binom{n}{k} = \binom{n}{n-k}$, those possible even integers we need to consider such that $\nu_p\left(\binom{n}{k}\right) = 0$ are $k = p^i+1,\ p^j+1,$ and $p^j + p^i = p^i(p^{j-i}+1)$. We know that 2 is a common divisor of n and k. If there is another common divisor $d \geq 2$ of $n/2$ and $k/2$, then we have $\gcd(n, k) > 2$ and thus $\binom{n}{k} \notin A_2(n)$. Note that $p \mid \gcd A_2(n)$ if and only if for each $k \in \{p^i+1,\ p^j+1,\ p^j+p^i\},$ there exists $d \geq 2$ such that

$$d \,\Big|\, \frac{n}{2}, \text{ and } d \,\Big|\, \frac{k}{2}.$$

For $k = p^i + 1$, the above condition implies

$$d \,\Big|\, \left(\frac{n}{2} - \frac{k}{2}\right) = p^j\left(\frac{p^{t-j}+1}{2}\right).$$

Thus, $d \mid (p^{t-j}+1)/2$ since p cannot be divisible by d. This implies that d would be a common divisor of $\bar{n}/2$ and $(p^{t-j}+1)/2$. The similar argument can be applied for the cases $k = p^j+1,$ and $p^j + p^i = p^i(p^{j-i}+1)$. These three conditions correspond to $p \mid \gcd A_2(\bar{n})$ and the proof completes. □

Remark 2 Let $n = p^t + p^j + p^i + 1 (t > j > i > 0)$. Taking $k = 2p^{t-1},$ we obtain $\binom{n}{k} \in A_2(n)$ and

$$\nu_p\left(\binom{n}{2p^{t-1}}\right) = 1,$$

by Kummer's theorem. Thus, $\nu_p(\gcd A_2(n)) \leq 1$. In light of Proposition 3, it follows that $\nu_p(\gcd A_2(n)) = 1$ if and only if $\nu_p(\gcd A_2(\bar{n})) = 1$. Moreover, we have $p \nmid \gcd A_2(n)$ if and only if $p \nmid \gcd A_2(\bar{n})$.

Let $n = p^t + p^j + p^i + 1 (t > j > i > 0)$. We say the pair (i, j) is admissible to $n = p^t + p^j + p^i + 1$ if $\gcd(n, k) > 2$ for all possible even integers k's with $\nu_p\left(\binom{n}{k}\right) = 0$. This terminology helps us determine whether $\nu_p(\gcd A_2(n))$ is 0 or 1 by Remark 2. It also tells us that a pair (i, j) is admissible to $n = p^t + p^j + p^i + 1$ if and only if $(t-j, t-i)$ is an admissible pair. We say that n is self-symmetry about p if $n = \bar{n}$. So it follows $t = i + j$ if n is self-symmetry about p. That is,

$$n = p^{i+j} + p^j + p^i + 1 = (p^j+1)(p^i+1).$$

In this case, the only possible even integer we need to consider with $\nu_p\left(\binom{n}{k}\right) = 0$ is $k = p^j + p^i$. For this k, note that

$$\gcd(n, k) = \gcd(p^{i+j}+1,\ p^i(p^{j-i}+1)) = \gcd(p^{i+j}+1,\ p^{j-i}+1).$$

With the help of (4), we have $\gcd(n, k) > 2$ if and only if $\nu_2(i+j) = \nu_2(j-i)$.

Proposition 4 For self-symmetry $n = p^t + p^j + p^i + 1,$ we have $\nu_p(\gcd A_2(n)) = 1$ if and only if $\nu_2(i+j) = \nu_2(j-i)$.

Proof. We only need to considerc when $k = p^j + p^i$. From the above discussion, we have $\gcd(n, k) > 2$ if and only if $\nu_2(i+j) = \nu_2(j-i)$. However, $\nu_p(\gcd A_2(n)) = 1 \Leftrightarrow \gcd(n, k) > 2$. So the result follows. □

Now, we prove Theorem 4, the general case for $\sigma_p(n) = 4$.

Proof of Theorem 4 Let $n = p^{t_1} + p^{t_2} + p^{t_3} + 1$. Note that $\nu_p(\gcd A_2(n)) = 1$ if and only if the pair (t_2, t_3) is admissible. That is, all possible even integers k's with $\nu_p\left(\binom{n}{k}\right) = 0$, which are $k = p^{t_2} + p^{t_3}$, $p^{t_2} + 1$, and $k = p^{t_3} + 1$, must satisfy $\gcd(n, k) > 2$. For example, if $k = p^{t_2} + p^{t_3}$, we have $\gcd(n, k) = \gcd(p^{t_1} + 1, p^{t_2} + p^{t_3}) = \gcd(p^{t_1} + 1, p^{t_2 - t_3} + 1)$. According to (4) in Corollary 1, these three conditions are equivalent to the simultaneous equations

$$\nu_2(t_1) = \nu_2(t_2 - t_3), \ \nu_2(t_2) = \nu_2(t_1 - t_3), \text{ and } \nu_2(t_3) = \nu_2(t_1 - t_2).$$

Hence, the necessary and sufficient conditions for $v_p(\gcd A_2(n)) = 1$ are

$$a_1 = \nu_2(2^{a_2}u_2 - 2^{a_3}u_3), \ a_2 = \nu_2(2^{a_1}u_1 - 2^{a_3}u_3), \text{ and } a_3 = \nu_2(2^{a_1}u_1 - 2^{a_2}u_2).$$

Without loss of generality, we may assume that $a_1 = \max\{a_1, a_2, a_3\}$. From the second and third equations given above, we obtain

$$a_2 \geq \min\{a_1, a_3\} = a_3, \ a_3 \geq \min\{a_1, a_2\} = a_2,$$

and thus $a_2 = a_3$. In addition, we have

$$a_1 = \nu_2(2^{a_2}u_2 - 2^{a_3}u_3) = a_2 + \nu_2(u_2 - u_3).$$

The proof is done. □

Remark 3 We might rephrase Theorem 4 in the following equivalent form: For $n = p^t + p^j + p^i + 1$ $(t > j > i > 0)$, we have $\nu_p(\gcd A_2(n)) = 1$ if and only if $t \sim_p (j-i)$, $j \sim_p (t-i)$, and $i \sim_p (t-j)$. In other words, for n is self-symmetry about p, a pair (i, j) is admissible if and only if $(i+j) \sim_p (j-i)$, if and only if $\nu_2(i+j) = \nu_2(j-i)$. This is exactly what Proposition 4 says. Notice that, by Theorem 4, there are infinitely many admissible pairs.

Example 1). Let us look at few examples. For the positive integer n_1 of the form $n_1 = p^{66} + p^{38} + p^{28} + 1 = (p^{38} + 1)(p^{28} + 1)$, we see that n is self-symmetry about p and $\nu_2(66) = \nu_2(38 - 28) = 1$. Hence $\nu_p(\gcd A_2(n_1)) = 1$ by Proposition 4.

2). Let $n_2 = p^{53} + p^{24} + p^{13} + 1$. We have $\nu_2(53) = \nu_2(13) = 0$ and $\nu_2(24) = 3$. Also, we have $\nu_2(53 - 13) = \nu_2(40) = 3$. Hence by Theorem 4, we have $\nu_p(\gcd A_2(n_2)) = 1$.

3). Let n_3 = 823,600, we have $n_3 - 1$ = 823,599 = $3^2 \cdot 7 \cdot 17 \cdot 769$, and

$$n_3 = (1, 302, 1)_{769}$$

$$= (9, 14, 10, 14, 1)_{17}$$

$$= (1, 0, 0, 0, 0, 1, 1, 1)_7$$

$$= (1, 1, 1, 2, 2, 1, 1, 2, 0, 2, 2, 0, 1)_3.$$

By Kummer's theorem, we see that 3, 17 and 769 can not be a prime divisor of $\gcd(A_2(823600))$. Now, $n_3 = 7^7 + 7^2 + 7^1 + 1$ satisfies conditions in Theorem 4, thus $\nu_7(\gcd A_2(823600)) = 1$ and indeed $\gcd A_2(823600) = \frac{823600}{2} \cdot 7 = 2882600$.

(iii) Now suppose that $s = \sigma_p(n) > 4$. We should demonstrate two specific consequences of this case. The first one is a special case for $s = 6$.

Proposition 5 Let n, a, t_1, and t_2 be positive integers. If $n = (p^a + 1)(p^{t_1} + p^{t_2} + 1)$ with $t_1 > t_2$, then we have $p \nmid \gcd A_2(n)$.

Proof. Assume that p is a prime divisor of $\gcd A_2(n)$. For any even integer k with $\nu_p\left(\binom{n}{k}\right) = 0$, we must have $\gcd(n, k) > 2$. Take $k_1 = p^{t_1} + 1$. Since $\nu_p\left(\binom{n}{k_1}\right) = 0$, we have

$$\gcd(k_1, n) = \gcd(p^{t_1} + 1, (p^a + 1)(p^{t_1} + p^{t_2} + 1)) = \gcd(p^{t_1} + 1, p^a + 1) > 2.$$

By Corollary 1, it implies that $\nu_2(t_1) = \nu_2(a)$. Denote this value $\nu_2(a)$ by m.

In the same way, we can consider $k_2 = p^{t_2} + 1$, $k_3 = p^{t_1} + p^{t_2}$ and then derive $\nu_2(t_2) = \nu_2(a)$ and $\nu_2(t_1 - t_2) = \nu_2(a)$, respectively. Say $t_1 = 2^m u_1$, and $t_2 = 2^m u_2$ with odd integers $u_1 > u_2$. However, we see that $\nu_2(t_1 - t_2) = m + \nu_2(u_1 - u_2) > m$, a contradiction. Hence we have $p \nmid \gcd A_2(n)$. □

Before proving the next result, we need a lemma that is interesting in its own right.

Lemma 2 Let n and d be positive integers, and p be an odd prime. Let $n = (c_t, c_{t-1}, \ldots, c_0)_p$. If $p^\ell + 1 \equiv 0 \pmod{d}$, we have d is a divisor of n if and only if

$$d \left| \sum_{i=0}^{\lfloor \frac{t}{\ell} \rfloor} (-1)^i (c_{i\ell+\ell-1}, c_{i\ell+\ell-2}, \ldots, c_{i\ell})_p, \right.$$

where $c_j = 0$ if $j > t$.

Proof. This follows by a direct computation:

$$\begin{aligned}
& n \equiv 0 \pmod{d} \\
\Leftrightarrow\ & (c_t, c_{t-1}, \ldots, c_0)_p \equiv 0 \pmod{d} \\
\Leftrightarrow\ & (c_t, c_{t-1}, \ldots, c_{\ell\lfloor \frac{t}{\ell} \rfloor})_p \cdot p^{\ell\lfloor \frac{t}{\ell} \rfloor} \\
& + \left(c_{\ell\lfloor \frac{t}{\ell} \rfloor - 1}, c_{\ell\lfloor \frac{t}{\ell} \rfloor - 2}, \ldots, c_{\ell(\lfloor \frac{t}{\ell} \rfloor - 1)}\right)_p \cdot p^{\ell\left(\lfloor \frac{t}{\ell} \rfloor - 1\right)} \\
& + \cdots + (c_{\ell-1}, c_{\ell-2}, \ldots, c_0)_p \equiv 0 \pmod{d}
\end{aligned}$$

$$\Leftrightarrow (c_t, c_{t-1}, \ldots, c_{\ell\lfloor\frac{t}{\ell}\rfloor})_p \cdot (-1)^{\ell\lfloor\frac{t}{\ell}\rfloor}$$

$$+ \left(c_{\ell\lfloor\frac{t}{\ell}\rfloor-1}, c_{\ell\lfloor\frac{t}{\ell}\rfloor-2}, \ldots, c_{\ell(\lfloor\frac{t}{\ell}\rfloor-1)}\right)_p \cdot (-1)^{\ell\left(\lfloor\frac{t}{\ell}\rfloor-1\right)}$$

$$+ \cdots + (c_{\ell-1}, c_{\ell-2}, \ldots, c_0)_p \equiv 0 \pmod{d}$$

$$\Leftrightarrow \sum_{i=0}^{\lfloor\frac{t}{\ell}\rfloor} (-1)^i (c_{i\ell+\ell-1}, c_{i\ell+\ell-2}, \ldots, c_{i\ell})_p \equiv 0 \pmod{d}.$$

□

We are now in a position to prove our second main result: Theorem 5.

Proof of Theorem 5 Suppose that s is not a power of 2. That is, $s = 2^a u$ with $a = \nu_2(s)$ and $u > 1$. We set $k = p^{2^a} + 1$. On one hand, if $d \mid \gcd(k, n)$, by Lemma 2, we have

$$d \mid n \Leftrightarrow d \left| \sum_{i=0}^{u-1} (-1)^i (\underbrace{1, 1, \ldots, 1}_{2^a})_p \right.$$

$$\Leftrightarrow d \left| (-1)^i (\underbrace{1, 1, \ldots, 1}_{2^a})_p \right.$$

$$\Leftrightarrow d \left| p^{2^a-1} + p^{2^a-2} + \cdots + p + 1 \right.$$

$$\Leftrightarrow d \left| (p+1)(p^2+1)(p^4+1)\cdots(p^{2^{a-1}}+1). \right.$$

On the other hand, by Corollary 1, we have

$$\gcd\left(p^{2^i}+1, p^{2^a}+1\right) = 2$$

for any positive integer $i < a$. In addition, we get

$$\gcd\left(p^{2^a}+1, p^{2^a-1} + p^{2^a-2} + \cdots + p + 1\right) = 2,$$

since $p^{2^a} + 1 \equiv 2 \pmod 4$. That is to say $\gcd(k, n) = 2$. It implies that $\binom{n}{k} \in A_2(n)$ and, by Kummer's theorem, $\nu_p\left(\binom{n}{k}\right) = 0$. Hence, we conclude that $p \nmid \gcd A_2(n)$ and $\nu_p(\gcd A_2(n)) = 0$.

If $b = 2$, then we have $s = 4$ and $n = p^3 + p^2 + p + 1 = (p^2+1)(p+1)$. Thus, n is self-symmetry about p. By proposition 3, it is easy to see that $3 \sim_p 1$. So we obtain $\nu_p(\gcd A_2(n)) = 1$ if $b = 2$.

Suppose $b=3$ and $p\equiv 1 \pmod 4$. We have $s=8$ and $n=(1,1,1,1,1,1,1,1)_p\equiv 0 \pmod 4$. Since $\binom{n}{k}=\binom{n}{n-k}$, we need to consider the cases $\sigma_p(k)=2, 4$ with $\nu_p\left(\binom{n}{k}\right)=0$. For each integer k with $\sigma_p(k)=4$ and $\nu_p\left(\binom{n}{k}\right)=0$, k is divisible by 4 since $p\equiv 1 \pmod 4$. Now, we consider the remaining case when $\sigma_p(k)=2$. Notice that $n=\frac{p^8-1}{p-1}=(p+1)(p^2+1)(p^4+1)$. Each k with $\sigma_p(k)=2$ and $\nu_p\left(\binom{n}{k}\right)=0$ can be written as $k=p^j+p^i=p^i(p^{j-i}+1)$ $(7\geq j>i\geq 0)$. Then we have $\gcd(n,k)=\gcd\left((p+1)(p^2+1)(p^4+1),\, p^{j-i}+1\right)$ and, by Corollary 1, we further have

$$\begin{cases} (p+1)\mid \gcd(n,k) & \text{, if } j-i \text{ is odd,} \\ (p^2+1)\mid \gcd(n,k) & \text{, if } j-i=2,6, \\ (p^4+1)\mid \gcd(n,k) & \text{, if } j-i=4. \end{cases}$$

which implies $\gcd(n,k)>2$ if $\sigma_p(k)=2$ with $\nu_p\left(\binom{n}{k}\right)=0$. That is, we show that $\gcd(n,k)>2$ for all k with $\nu_p\left(\binom{n}{k}\right)=0$ which is equivalent to $\nu_p\left(\gcd A_2(n)\right)=1$.

Assume $b=3$ and $p\equiv 3 \pmod 4$. We have $s=8$ and $n=(p+1)(p^2+1)(p^4+1)\equiv 0 \pmod 4$. If we can find a positive even integer k such that $\gcd(n,k)=2$ and $\nu_p\left(\binom{n}{k}\right)=0$, then we can conclude that $\nu_p\left(\gcd A_2(n)\right)=0$. Take $k=p^4+p^2+p+1$ and we will show that it is indeed such an example. Note that $k\equiv 2 \pmod 4$ so that $4\nmid \gcd(k,n)$. Apply the result in Corollary 1, it is easy to see that

$$\gcd(k,\, p^{2^c}+1)=2,$$

for $c\in\{0,1,2\}$, and hence $\gcd(k,n)=2$ and $\nu_p\left(\binom{n}{k}\right)=0$.

Finally, for $b\geq 4$ and $s=2^b$, we have

$$n=\frac{p^{2^b}-1}{p-1}=\prod_{\substack{d\mid 2^b \\ d\neq 1}}\Phi_d(p)=(p+1)(p^2+1)\cdots(p^{2^{b-1}}+1),$$

where $\Phi_d(x)$ is the dth cyclotomic polynomial. Consider

$$k=p(p+1)(p^2+1)(p^4+1)\cdots(p^{2^{b-3}}+1)+p^{2^{b-1}}+1$$

$$=p^{2^{b-1}}+p^{2^{b-2}}+p^{2^{b-2}-1}+\cdots+p^2+p+1.$$

Notice that $\nu_2(k)=1$ since $k\equiv 2 \pmod 4$. For $0\leq c\leq b-3$, we have

$$\gcd(k,\, p^{2^c}+1)=\gcd(p^{2^{b-1}}+1,\, p^{2^c}+1)=2.$$

Furthermore, by the Euclidean algorithm we have

$$\begin{aligned}\gcd(k,\, p^{2^{b-2}}+1) &= \gcd(p(p+1)\cdots(p^{2^{b-3}}+1)+2,\, p^{2^{b-2}}+1)\\ &= \gcd(p^{2^{b-2}}+p^{2^{b-2}-1}+\cdots+p+2,\, p^{2^{b-2}}+1)\\ &= \gcd(p^{2^{b-2}-1}+p^{2^{b-2}-2}+\cdots+p+1,\, p^{2^{b-2}}+1)\\ &= \gcd(p^{2^{b-2}-1}+p^{2^{b-2}-2}+\cdots+p+1,\, 2) = 2,\end{aligned}$$

and

$$\begin{aligned}\gcd(k,\, p^{2^{b-1}}+1) &= \gcd(p(p+1)\cdots(p^{2^{b-3}}+1),\, p^{2^{b-1}}+1)\\ &= \gcd((p+1)(p^2+1)\cdots(p^{2^{b-3}}+1),\, p^{2^{b-1}}+1).\end{aligned}$$

Let $Q=(p+1)(p^2+1)\cdots(p^{2^{b-3}}+1)$. Note that $(p^{2^{b-1}}+1)-(p-1)Q(p^{2^{b-2}}+1)=2$, together with the above equaions, we get

$$\gcd(k,\, p^{2^{b-1}}+1) = \gcd(Q,\, p^{2^{b-1}}+1) = \gcd(Q,\, 2) = 2.$$

From this, we conclude that $\nu_2(k)=1$ and $\gcd(k,\, p^{2^c}+1)=2$ for $0\le c\le b-1$. It implies $\gcd(k,n)=2$, $\binom{n}{k}\in A_2(n)$, and then $\nu_p(\gcd A_2(n))=0$. □

3. Concluding remarks, and open problems

Determining the exact value of $\gcd B_2(n)$ becomes more difficult than that of $\gcd A_2(n)$ for us. In this paper we just deal with a special case for $\gcd B_2(n)$ and leave the problems to those readers who are interested in.

Proposition 6 For any even integer n with $n-1=p^t$ $(t>0)$, an odd prime power, we have $\gcd B_2(n)=(n/2)\cdot p$.

Proof. We need only to prove that, in the case $n-1$ is a prime power, $b(n)=1$ since then by Proposition 1 the result follows. By the well-known solution of Catalan's equation, the integer n cannot be a prime power. So the prime power p^t is the smallest prime power less than or equal to n. It implies that $b(n)=n-p^t=1$. □

Remark 4 We can avoid using the result about the solution of Catalan's equation. We give a direct proof of the integer n with $n-1=p^t$ cannot be a prime power. Assume otherwise, such as $n=q^w$, n is a prime power. Thus, $q^w-p^t=1$. It is obvious that p and q must be of different parity, so it implies $q=2$ since n is even. Now, $2^w=p^t+1$. If t is odd, we get an odd divisor, namely $p^{t-1}-p^{t-2}+\cdots-p+1$, of 2^w which is absurd. Hence t must be even. Let $t=2r$ and $p^r=2m+1$. From

$$2^w=(p^r)^2+1=(2m+1)^2+1=4m^2+4m+2\equiv 2 \pmod 4,$$

it only holds when $w = 1$, and then $r = 0$. So we have $p = 1$, which is again absurd.

For those positive integers n's satisfying $b(n) = 0$, that is to say $n = p^m$ $(m \geq 1)$ is a prime power, we have

$$\gcd B_1(n) = \gcd\left(\left\{\binom{n}{k} : 0 < k < n,\ \gcd(k, n) = 1\right\}\right)$$

$$= \gcd\left(\left\{\binom{n}{k} : 1 \leq k \leq n,\ \gcd(k, p) = 1\right\}\right).$$

So by Albree's result (1), we get

$$\gcd B_1(p^m) = \gcd\left(\left\{\binom{p^m}{k} : 1 \leq k \leq p^m,\ \gcd(k, p) = 1\right\}\right) = p^m.$$

Consider $\gcd B_2(n)$ with those n's satisfying $b(n) = 0$. We require that n is even in this case, and thus $n = 2^m$ $(m \geq 1)$. By McTague's theorem (Theorem 2), we obtain that $p \mid \gcd B_2(2^m)$ if and only if $\sigma_p(2^m) = 2$, where p is an odd prime so that $p \mid (2^m - 1)$. Hence it must be the case $2^m = p^t + 1$ and, if we can solve this equation $2^m = p^t + 1$ in (m, p, t), by Proposition 1, $\gcd B_2(2^m) = \gcd A_2(2^m) = 2^{m-1} \cdot p$. For example, $2^7 = 127 + 1$, we have $\gcd B_2(128) = \gcd A_2(128) = (128/2) \cdot 127 = 8{,}128$. Let $n = 2^{12} = 4{,}096$. Clearly there is no odd prime power p^t such that $p^t + 1 = 4{,}096$. Therefore, $\gcd B_2(4{,}096) = \gcd A_2(4{,}096) = 2{,}048$.

In general, if $b(n) \geq 1$, we have no idea about the exact value of $\gcd B_2(n)$. For example, $\gcd B_2(58) = 29 \cdot 53$ but $\gcd A_2(58) = 58/2 = 29$. Another example $\gcd B_2(40) = 2^2 \cdot 3 \cdot 5 \cdot 19 \cdot 37$, however $\gcd A_2(40) = 2^2 \cdot 3 \cdot 5$. Of above two examples, $b(58) = 5$, and $b(40) = 3$. We might ask the following questions. How to determine the value of $\gcd B_2(n)$? Or, in general, what are the values of $\gcd A_d(n)$ and $\gcd B_d(n)$ for any positive integer $d \geq 2$ and for any positive integer n? At least, we have a simple observation as below.

Proposition 7 If $n = p^e + b(n)$, we have $p \mid \gcd B_d(n)$ for any integer $d \geq 1$.

Proof. In light of Theorem 3, p is a prime common divisor of elements of the set

$$\left\{\binom{n}{k} : b(n) < k < n - b(n)\right\},$$

and then p is a prime common divisor of elements of $B_d(n)$. Hence, the result follows obviously. □

By a similar argument for Proposition 1, we obtain easily that $n/2$ must be a common divisor of elements of the set $B_2(n)$. Hence, by the previous proposition, we then have

$$\frac{n}{2} \cdot p \ \Big|\ \gcd B_2(n),$$

where $n = p^e + b(n)$.

Here is a brief summary of this paper. In order to determine the value of $\gcd A_2(n)$, we divide into three subcases according to the even integer $\sigma_p(n) = s$. If $s = 2$, we conclude that n is the form of $n = p^t + 1$ and have $\gcd A_2(n) = (n/2) \cdot p$. When $s = 4$, we let $n = p^t + p^j + p^i + 1$ $(t > j > i > 0)$, and we have $\nu_p(\gcd A_2(n)) = 1$ if and only if $t \sim_p (j - i)$, $j \sim_p (t - i)$, and $i \sim_p (t - j)$. For $s > 6$ we obtain two specific results. Especially, the situation when $n = (\underbrace{1, 1, \ldots, 1}_{s})_p$ is clear. Actually, our Theorem 5 states that $\nu_p(\gcd A_2(n)) = 1$ if and only if $s = 4$, or $s = 8$ and $p \equiv 1 \pmod 4$.

In addition, we propose the following two conjectures.

Conjecture 1 Among odd prime divisors of $n-1$, we have at most one prime p such that $\nu_p(\gcd A_2(n)) = 1$.

If Conjecture 1 holds, we should paraphrase Theorem 4 as: For $n = p^{t_1} + p^{t_2} + p^{t_3} + 1$ $(t_1 > t_2 > t_3 > 0)$, let $a_m = v_2(t_m)$, we write $t_m = 2^{a_m} u_m$ with odd integers u_m for $m = 1, 2, 3$. Then we have $\gcd A_2(n) = (n/2) \cdot p$ if and only if $a_i = a_j < a_k$ for $\{i, j, k\} = \{1, 2, 3\}$ and $a_k = a_i + v_2(u_i - u_j)$. Similarly, if Conjecture 1 holds, the statement "$\nu_p(\gcd A_2(n)) = 0$" in Theorem 5 could be replaced by "$\gcd A_2(n) = n/2$"; and the statement "$\nu_p(\gcd A_2(n)) = 1$" in Theorem 5 could be replaced by "$\gcd A_2(n) = (n/2) \cdot p$".

Conjecture 2 If $\sigma_p(n) \neq 2$ and $\sigma_p(n) \equiv 2 \pmod 4$ for all odd primes $p \mid (n-1)$, we have $\gcd A_2(n) = n/2$.

Acknowledgement

The first author is supported by Fujian Natural Science grant No.2024J01362, and by Fuzhou University grant 0490-50011051, 0490-53007802. The second author is supported partially by the NSTC grant 111-2115-M-031-005-MY3.

Conflict of interest

The authors declare no competing financial interest.

References

[1] Singmaster D. Divisibility of binomial and multinomial coefficients by primes and prime powers. In: *A Collection of Manuscripts Related to the Fibonacci Sequence*. Santa Clara, California: The Fibonacci Association, University of Santa Clara; 1980. p.98-113.

[2] Granville A. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. *Organic Mathematics*. 1997; 20: 253-276. Available from: https://dms.umontreal.ca/~andrew/Binomial/.

[3] Kummer EE. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen [On the supplementary clauses to the general laws of reciprocity]. *Journal for Pure and Applied Mathematics*. 1852; 44: 93-146. Available from: https://doi.org/10.1515/crll.1852.44.93.

[4] Ram B. Common factors of $n!/m!(n-m)!$ $(m = 1, 2, \ldots, n-1)$. *The Journal of the Indian Mathematical Club (Madras)*. 1909; 1: 39-43.

[5] Mendelsohn NS. Divisors of binomial coefficients. *The American Mathematical Monthly*. 1971; 78: 201-202.

[6] Albree J. The gcd of certain binomial coefficients. *Mathematics Magazine*. 1972; 45: 259-261.

[7] Joris H, Oestreicher C, Steinig J. The greatest common divisor of certain sets of binomial coefficients. *Journal of Number Theory*. 1985; 21(1): 101-119. Available from: https://doi.org/10.1016/0022-314X(85)90013-7.

[8] Hong S. The greatest common divisor of certain binomial coefficients. *Mathematical Reports*. 2016; 354(8): 756-761.

[9] McTague C. On the greatest common divisor of binomial coefficients. *The American Mathematical Monthly*. 2017; 124(4): 353-356.

[10] Soulé C. Secant varieties and successive minima. *Journal of Algebraic Geometry*. 2004; 13: 323-341.

[11] Xiao J, Yuan P, Lin X. The greatest common divisor of certain set of binomial coefficients. *Mathematical Theory and Applications*. 2022; 42(1): 85-91.