The Greatest Common Divisor of Certain Set of Binomial Coefficients

Xiao Jiaqi Yuan Pingzhi* Lin Xucan

(School of Mathematical Science, South China Normal University, Guangzhou 510631, China)

Abstract In this paper, we prove that if $n \geq 4$ and $a \geq 0$ are integers satisfying $a < \frac{n}{3}$, then

$$\gcd\left(\left\{\binom{n}{k} : a < k < n-a\right\}\right) = \prod_{n=p^m+b(n,p),\ 0\leq b(n,p)\leq a,} p,$$

where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, and the product in the right hand side runs through all primes p such that $n = p^m + b(n,p), m \in \mathbb{N}$ and $0 \leq b(n,p) \leq a$. As an application of our result, we give an answer to a problem in Hong [3].

Key words Binomial coefficient Greatest common divisor

一些二项式系数的最大公因数

肖嘉琪 袁平之 * 林序灿

(华南师范大学数学科学学院, 广州, 510631)

摘 要 本文证明: 若 $n \geq 4$ 和 $a \geq 0$ 为整数且满足 $a < \frac{n}{3}$, 则

$$\gcd\left(\left\{\binom{n}{k} : a < k < n-a\right\}\right) = \prod_{n=p^m+b(n,p),\ 0\leq b(n,p)\leq a,} p,$$

其中 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, 右边的连乘积遍历所有满足 $n = p^m + b(n,p), m \in \mathbb{N}$ 和 $0 \leq b(n,p) \leq a$ 的素数 p. 作为上述结论的一个应用, 我们回答洪 [3] 文中的一个问题.

关键词 二项式系数 最大公因数

1 Introduction

Let n and k be nonnegative integers. The binomial coefficient $\binom{n}{k}$ is defined by $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ if $k \leq n$, and is 0 otherwise. For any finite set S of integers, we denote the greatest common divisor of all the elements of S by $\gcd(S)$. For any prime p, we use $\nu_p(n)$ to denote the largest nonnegative integer e such that p^e divides n. Such $\nu_p(n)$ is called the normalized p-adic valuation of n. For any integer $n > 0$, let $b(n) \geq 0$ be the smallest integer b such that the set of binomial coefficients $\binom{n}{m}$, where $b < m < n-b$, has a (non-trivial) common divisor. In 1909, Ram [10] proved that for any $n > 1$ and any prime p,

$$\gcd\left(\left\{\binom{n}{k} : 1 \leq k \leq n-1\right\}\right) = \begin{cases} p, & \text{if } n = p^i \text{ for some } i > 0, \\ 1, & \text{otherwise.} \end{cases}$$

This work is supported by National Natural Science Foundation of China (No. 12171163)

Corresponding author: Yuan Pingzhi(1966–), Professor, PhD; E-mail: yuanpz@scnu.edu.cn

收稿日期: 2021 年 10 月 28 日

In 1985, a generalization of Ram's result is obtained in [5] by determining $d(n;r,s) = \gcd\left(\left\{\binom{n}{k} : r \le k \le s\right\}\right)$ for any $r \le s \le n$. However, the explicit formula for $d(n;r,s)$ is too complicated to be stated here. On the other hand, Mendelsohn et al. [9] showed that $\gcd\left(\left\{\binom{2n}{2k-1} : 1 \le k \le n\right\}\right) = 2^{1+\nu_2(n)}$. In 1972, Albree [1] generalized the result in [9] by showing that if p is a prime, then $\gcd\left(\left\{\binom{pn}{k} : 1 \le k \le pn, p \not| k\right\}\right) = p^{1+\nu_p(n)}$. In 2016, Hong [3] proved that

$$\gcd\left(\left\{\binom{mn}{k} : 1 \le k \le mn, \gcd(k,m) = 1\right\}\right) = m \prod_{p|\gcd(m,n)} p^{\nu_p(n)},$$

and proposed the following interesting problem:

Problem 1.1 Let $n \ge 2$ be an integer and $b(n)$ be defined as above. Find the explicit formula for

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

In 1859, Kummer [6] got the following result.

Theorem 1.1 For any integers $0 \le k \le n$ and any prime p:

$$\nu_p\left(\binom{n}{k}\right) = \sharp\{\text{carries when adding } k \text{ to } n-k \text{ in base } p\}.$$

By Kummer's theorem, $\nu_p\left(\binom{n}{k}\right) = 0$ if and only if there are no carries when adding k to $n-k$ in base p. This happens if and only if each base-p digit of k is no more than the corresponding base-p digit of n. Based on Kummer's theorem, McTague [8] showed that the greatest common divisor of the binomial coefficients $\binom{2n}{2}, \binom{2n}{4}, \cdots, \binom{2n}{2n-2}$, equals the products of all odd primes p such that $2n = p^i + p^j$, for some $i \le j$. McTague also obtained some other results in [8].

For any prime p, we denote the sum of the standard base-p digits of n by $\sigma_p(n)$, i.e. $\sigma_p(n) := \Sigma_{i=0}^{r} a_i$ if $n = \sum_{i=0}^{r} a_i p^i$ with $r \ge 0$ and a_i being integers such that $a_r > 0$ and $0 \le a_i \le p-1$ for all integers i with $0 \le i \le r$.

The main purpose of this paper is to give an answer to the above mentioned problem of Hong. We give an explicit formula for the greatest common divisor of the set of the binomial coefficients $\binom{n}{k}$, where k runs over all the integers between a and $n-a$. Let $n \ge 4$ be a positive integer. For any prime $p \le n$, let $p^m, m \in \mathbb{N}$ be the largest prime power of p which is less than or equal to n, and let $b(n,p) = n - p^m$, then $n = p^m + b(n,p), m \in \mathbb{N}$. The main result of this paper is as follows.

Theorem 1.2 Let $n \ge 4$ and $a \ge 0$ be integers with $a < \frac{n}{3}$. Then

$$\gcd\left(\left\{\binom{n}{k} : a < k < n-a\right\}\right) = \prod_{n=p^m+b(n,p),\ 0\le b(n,p)\le a,} p,$$

where the product runs through all primes p such that $n = p^m + b(n,p), m \in \mathbb{N}$ and $0 \le b(n,p) \le a$.

By the result of [11], we know that $b(n) \le \frac{n}{4}$, $n = p^m + b(n)$ for some positive integer m. Moreover, p is the only prime with $n = p^m + b(n,p), m \in \mathbb{N}$ and $0 \le b(n) \le b(n,\ p)$. Therefore, as an immediate consequence of Theorem 1.2, we have the following result, which gives an answer to the above problem of Hong.

Corollary 1.1 For any integer $n > 0$, let $b(n) \geq 0$ be the smallest integer b such that the binomial coefficients $\binom{n}{k}$, where $b < k < n-b$, has a (non-trivial) common divisor. Then $n = p^m + b(n)$ for some prime p and positive integer m, $b(n) \leq \frac{n}{4}$ and

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

Remark 1.1 It is easy to check that

$$\nu_3\left(\gcd\left(\binom{9}{4}, \binom{9}{5}\right)\right) = 2$$

and $\gcd\left(\binom{27}{10}, \binom{27}{11}, \binom{27}{12}, \binom{27}{13}, \binom{27}{14}, \binom{27}{15}, \binom{27}{16}, \binom{27}{17}\right) = 3^2 \times 5 \times 19 \times 23$, so $a < \frac{n}{3}$ in Theorem 1.1 is best possible in general.

The arrangement of the paper is follows: In the Section 2, we prove several preliminary lemmas. Then we use these lemmas to prove Theorem 1.2 in Section 3.

2 Preliminaries

In this section, we prove some lemmas that are needed in the proof of Theorem 1.2. The following Lemma is essential in the sequel.

Lemma 2.1 Let p be a prime and let $n \geq 2$, $e \geq 0$ and d be integers such that $1 \leq d \leq p-1$ and $n \geq dp^e$. Then $\nu_p(\binom{n}{dp^e}) = t - e$, where $t = \max\{\nu_p(n-i),\ i = 0, 1, \cdots, dp^e - 1\}$.

Proof Suppose that $t = \nu_p(n-i)$ for some integer i with $0 \leq i \leq dp^e - 1$, then we have $n - i = up^t$, $\gcd(u, p) = 1$. Let $n = qp^e + r, 0 \leq r \leq p^e - 1$, then $0 \leq r \leq dp^e - 1$ and $\nu_p(n-r) = \nu_p(qp^e) \geq e$, hence $t \geq e$. Now

$$n(n-1)\cdots(n-dp^e+1) = (up^t+i)\cdots(up^t+1)(up^t)(up^t-1)\cdots(up^t-dp^e+i+1).$$

If $t > e$, since $\nu_p(j) \leq e < t$ for any j with $1 \leq j \leq dp^e - 1$, then we have

$$\nu_p(up^t + j) = \nu_p(j), \quad 1 \leq j \leq i \tag{2.1}$$

and

$$\nu_p(up^t - j) = \nu_p(j), \quad 1 \leq j \leq dp^e - i - 1. \tag{2.2}$$

If $t = e$ and $\nu_p(j) < e$ for any j with $0 \leq j \leq \max\{i, dp^e - i - 1\}$, then the above equalities (2.1) and (2.2) hold since $\nu_p(j) < t = e$. If $t = e$ and $\nu_p(j) = e$ for some j with $1 \leq j \leq \max\{i, dp^e - i - 1\}$, then $j = d_1 p^e, 1 \leq d_1 \leq d-1$ and $1 \leq d_1 p^e \leq dp^e - i - 1$. We claim that $\nu_p(up^e - j) = \nu_p(j) = e$. Otherwise, $\nu_p(up^e - j) = \nu_p(up^e - d_1 p^e) > e$. Take $i_1 = i + d_1 p^e$, then $i_1 = i + d_1 p^e \leq i + dp^e - i - 1 = dp^e - 1$ and $\nu_p(up^e - i_1) > e$, which contradicts to the definition of t. Hence $\nu_p(up^e - j) = \nu_p(j) = e$ and the above equalities (2.1) and (2.2) hold in this case.

Note that $\nu_p(s)=\nu_p(up^e-s)$ holds for all $s, 1\le s\le dp^e-1$. Hence

$$\begin{aligned}\nu_p(n(n-1)\cdots(n-dp^e+1)) = \quad & t+\sum_{j=1}^{i}\nu_p(up^t+j)+\sum_{s=1}^{dp^e-i-1}v_p(up^t-s)\\ =t+\sum_{j=1}^{i}\nu_p(j)+\sum_{s=1}^{dp^e-i-1}\nu_p(s) &= t+\sum_{j=1}^{i}\nu_p(j)+\sum_{j=i+1}^{dp^e-1}v_p(j)\\ =t+\sum_{j=1}^{dp^e-1}v_p(j) &= t+v_p((dp^e)!)-e,\end{aligned}$$

it follows that $\nu_p(\binom{n}{dp^e})=t-e$. This completes the proof.

Remark 2.1 Let $d=1$ and $\nu_p(n)\ge e$. Then we get the result of Lemma 2.3 in Hong [3].

Lemma 2.2 ([4]) Let n and k be non-negative integers with $n\ge k$, and let p be a prime number. Then $\nu_p(\binom{n}{k})=\frac{\sigma(k)+\sigma(n-k)-\sigma_p(n)}{p-1}$.

Lemma 2.3 Let $n\ge 2, a$ be positive integers with $a<n/2$ and let p be a prime. If $n=p^m+b(n,p), m\in\mathbb{N}$ and $0\le b(n,p)\le a$, then $\sigma_p(k)+\sigma_p(n-k)\ge p+\sigma_p(b(n,p))$ for every positive integer k with $a<k<n-a$.

Proof By the assumptions, we have

$$n=p^m+b(n,p),\quad b(n,p)\le\max\{p^m-1,\,a\}.$$

Hence for any positive integer k with $a<k<n-a$, we have $a<k, n-k<p^m$. Let $b(n,p)=\sum_{i=0}^{m-1}a_ip^i$, $k=\sum_{i=0}^{m-1}b_ip^i$, $n-k=\sum_{i=0}^{m-1}c_ip^i$, $0\le a_i,\,b_i,\,c_i\le p-1$ be the base p expansions of $b(n,p)$, k and $n-k$, respectively. Then

$$b_{m-1}+c_{m-1}=a_{m-1}+p\quad\text{or}\quad b_{m-1}+c_{m-1}=a_{m-1}+p-1.$$

Let $b'=\sum_{i=0}^{m-2}a_ip^i, k'=\sum_{i=0}^{m-2}b_ip^i, l'=\sum_{i=0}^{m-2}c_ip^i$. If $b_{m-1}+c_{m-1}=a_{m-1}+p$, then $b'=k'+l'$. Hence $\sigma_p(k)=b_{m-1}+\sigma_p(k')$, $\sigma_p(n-k)=c_{m-1}+\sigma_p(l')$, $\sigma_p(b(n,p))=a_{m-1}+\sigma_p(b')$. By Lemma 2.2, we obtain that

$$0\le\nu_p\left(\binom{b'}{k'}\right)=\frac{\sigma_p(k')+\sigma_p(l')-\sigma_p(b')}{p-1},$$

hence $\sigma_p(k')+\sigma_p(l')-\sigma_p(b')\ge 0$. It follows that

$$\begin{aligned}&\sigma_p(k)+\sigma_p(n-k)-1-\sigma_p(b(n,p))\\ &=b_{m-1}+\sigma_p(k')+c_{m-1}+\sigma_p(l')-1-a_{m-1}-\sigma_p(b')\\ &=a_{m-1}+p+\sigma_p(k')+\sigma_p(l')-1-a_{m-1}-\sigma_p(b')\\ &=p-1+\sigma_p(k')+\sigma_p(l')-\sigma_p(b')\\ &\ge p-1.\end{aligned}$$

That is, $\sigma_p(k)+\sigma_p(n-k)\geq p+\sigma_p(b(n,p))$. If $b_{m-1}+c_{m-1}=a_{m-1}+p-1$, then $k^{'}+l^{'}=b^{'}+p^{m-1}$. By Lemma 2.2 again, we get

$$0\leq \nu_p\left(\binom{b^{'}+p^{m-1}}{k^{'}}\right)=\frac{\sigma_p(k^{'})+\sigma_p(l^{'})-\sigma_p(b^{'}+p^{m-1})}{p-1},$$

so

$$\sigma_p(k^{'})+\sigma_p(l^{'})-\sigma_p(b^{'}+p^{m-1})\geq 0.$$

Thus,

$$\begin{aligned}&\sigma_p(k)+\sigma_p(n-k)-1-\sigma_p(b(n,p))\\&=b_{m-1}+\sigma_p(k^{'})+c_{m-1}+\sigma_p(l^{'})-1-a_{m-1}-\sigma_p(b^{'})\\&=p-1+\sigma_p(k^{'})+\sigma_p(l^{'})-1-\sigma_p(b^{'})\\&=p-1+\sigma_p(k^{'})+\sigma_p(l^{'})-\sigma_p(b^{'}+p^{m-1})\geq p-1.\end{aligned}$$

That is, $\sigma_p(k)+\sigma_p(n-k)\geq p+\sigma_p(b(n,p))$. This completes the proof.

3 Proof of Theorem 1.2

In this section, we prove Theorem 1.2.

Proof Suppose that p is a prime such that $n=p^m+b(n,p), m\in\mathbb{N}$ and $b(n,p)\leq a$, we will first show that $p\mid\binom{n}{k}$ for every k with $a<k<n-a$. Since $b(n,p)\leq a<\frac{n}{3}$, we have $b(n,p)<p^m$. Note that $a<k<n-a$, so $a<k, n-k<p^m$. Let $b(n,p)=\sum_{i=0}^{m-1}a_ip^i$, $k=\sum_{i=0}^{m-1}b_ip^i$, $n-k=\sum_{i=0}^{m-1}c_ip^i$, $0\leq a_i,\ b_i,\ c_i\leq p-1$ be the base p expansions of $b(n,p)$, k and $n-k$, respectively. Then by Lemmas 2.2 and 2.3, we obtain that

$$\begin{aligned}&\nu_p\left(\binom{n}{k}\right)\\&=\frac{\sigma_p(k)+\sigma_p(n-k)-\sigma_p(n)}{p-1}\\&=\frac{\sigma_p(k)+\sigma_p(n-k)-\sigma_p(b(n,p))-1}{p-1}\geq 1.\end{aligned}$$

Hence $p\mid\binom{n}{k}$ for every k with $a<k<n-a$.

Next we show that $\nu_p(\binom{n}{k})=1$ for some positive integer k with $a<k<n-a$. We divide the proof into two cases according to $m=1$ and $m>1$.

Case 1: $m=1$. It follows that $n=p+b(n,p)$. Since $b(n,p)\leq a<\frac{n}{3}$, we have $a+1<p$. Take $k=a+1$, then $a<k<n-a$, and $\nu_p(\binom{n}{a+1})=1$ by Lemma 2.1.

Case 2: $m>1$. Let $n=qp^{m-1}+r, 0\leq r<p^{m-1}$, then $q\geq p\geq 2$. If $q=2s,\ s\geq 1$, we take $k=sp^{m-1}$. We have $n=2sp^{m-1}+r<(2s+1)p^{m-1}$, $sp^{m-1}>\frac{sn}{2s+1}\geq\frac{n}{3}>a$, $sp^{m-1}=\frac{n-r}{2}<\frac{n}{2}<n-a$ and $\nu_p(\binom{n}{sp^{m-1}})=1$ by Lemma 2.1.

If $q = 3$, we take $k = 2p^{m-1}$. In this case, $n = 3p^{m-1} + r < 4p^{m-1}$, $2p^{m-1} > \frac{n}{2} > a$, $2p^{m-1} = \frac{2(n-r)}{3} \leq \frac{2n}{3} < n - a$ and $\nu_p(\binom{n}{2p^{m-1}}) = 1$ by Lemma 2.1 again.

If $q = 2s + 1, s > 1$, we take $k = sp^{m-1}$. Now $n = (2s + 1)p^{m-1} + r < (2s + 2)p^{m-1}$, $sp^{m-1} > \frac{sn}{2s+2} \geq \frac{n}{3} > a$. $sp^{m-1} = \frac{s(n-r)}{2s+1} < \frac{n}{2} < n - a$, and $\nu_p(\binom{n}{sp^{m-1}}) = 1$ by Lemma 2.1.

To sum up, we have found a positive integer k such that $\nu_p(\binom{n}{k}) = 1$ and $a < k < n - a$.

Let $p < n$ be a prime such that $n = p^m + b(n, p), m \in \mathbb{N}$. Since p^m is the largest prime power of p which is less than or equal to n, we have $n = dp^m + r, 1 \leq d \leq (p-1)$ and $0 \leq r \leq p^m - 1$. If $b(n, p) \leq a$ does not hold, then we have $a < b(n, p) < p^m$ or $n = dp^m + r, 2 \leq d \leq (p - 1)$ and $0 \leq r \leq p^m - 1$. Now we show that there exists a positive integer k such that $a < k < n - a$ and $\nu_p(\binom{n}{k}) = 0$.

If p is a prime such that $n = p^m + r, a < r < p^m$, then $a < p^m < n - a$ and $\nu_p\left(\binom{n}{p^m}\right) = 0$ by Lemma 2.1.

If p is a prime such that $n = dp^m + r, 2 \leq d \leq (p - 1)$ and $0 \leq r \leq p^m - 1$. For $d = 2s, 3, (2s + 1)(s > 1)$, we take $k = sp^m, 2p^m$ and sp^m, respectively. By the same argument as above, we have $a < k < n - a$ and $\nu_p\left(\binom{n}{k}\right) = 0$ by Lemma 2.1. Therefore, we have proved that for any prime p, $\nu_p\left(\gcd\left(\{\binom{n}{k} : a < k < n - a\}\right)\right) = 1$ if $n = p^m + b(n, p)$ and $b(n, p) < a$ and $\nu_p\left(\gcd\left(\{\binom{n}{k} : a < k < n - a\}\right)\right) = 0$ otherwise. It follows that

$$\gcd\left(\left\{\binom{n}{k} : a < k < n - a\right\}\right) = \prod_{n=p^m+b(n,p),0\leq b(n,p)\leq a,} p,$$

where the product runs through all primes p such that $n = p^m + b(n, p), m \in \mathbb{N}$ and $0 \leq b(n, p) \leq a$. This completes the proof of Theorem 1.2.

References

[1] Albree J. The gcd of certain binomial coefficients[J]. Mathematics Magazine. 1972, 45:259-261.

[2] Granville A. Arithmetic properties of binomial coefficients I: Binomial coefficients modulo prime powers[M]. Burnaby: Organic mathematics, 1995.

[3] Hong S. The greatest common divisor of certain binomial coefficients[J]. Comptes rendus-Mathématique, 2016, 354: 756-761.

[4] Kenneth F. A classical introduction to modern number theory[M]. New York: Springer-Verlag, 1990.

[5] Joris H, Oestreicher C, Steinig J. The greatest common divisor of certain sets of binomial coefficients[J]. Journal of Number Theory, 1985, 21(1): 101-119.

[6] Kummer E E. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen[J], Journal für die Reine und Angewandte Mathematik, 1859, 56: 93-146.

[7] Mctague C. The Cayley plane and String bordism[J]. Geometry & Topology, 2014, 18(4): 2045-2078.

[8] Mctague C. On the greatest common divisor of binomial coefficients[J], American Mathematical Monthly, 2017, 124(4): 353-356.

[9] Mendelsohn N S. Divisors of binomial coefficients[J], American Mathematical Monthly, 1971, 78: 201-202.

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

[11] Soulè C. Secant varieties and successive minima[J]. Journal of Algebraic Geometry, 2004, 13: 323-341.