C. R. Acad. Sci. Paris, Ser. I 354 (2016) 756–761

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory

The greatest common divisor of certain binomial coefficients

Le plus grand commun diviseur de certains coefficients binomiaux

Siao Hong

Center for Combinatorics, Nankai University, Tianjin 300071, PR China

ARTICLE INFO

Article history:
Received 15 March 2016
Accepted after revision 8 June 2016
Available online 12 July 2016

Presented by the Editorial Board

ABSTRACT

Let m and n be positive integers. Let $\binom{m}{n} = \frac{m!}{n!(m-n)!}$ denote the binomial coefficient indexed by m and n, where $n!$ is the factorial of n. For any prime p, let $\nu_p(n)$ denote the largest nonnegative integer r such that p^r divides n. In this paper, we use the p-adic method to show the following identity:

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

This extends greatly the identities obtained by Mendelsohn et al. in 1971 and by Albree in 1972, respectively.

RÉSUMÉ

Soient m et n deux entiers positifs. Soit $\binom{m}{n} = \frac{m!}{n!(m-n)!}$ le coefficient binomial. Pour chaque nombre premier p, soit $\nu_p(n)$ le plus grand entier r tel que p^r divise n. Dans cet article, nous montrons l'identité suivante :

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

Ceci améliore les identités obtenues par Mendelsohn et al. en 1971 et par Albree in 1972.

1. Introduction

Let $n \ge 1$ and $k \ge 0$ be integers. The binomial coefficient, indexed by n and k, is as usual written as $\binom{n}{k}$, and can defined to be the coefficient of the x^k term in the polynomial expansion of the binomial power $(1+x)^n$. In other words, one has $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$, with $n!$ being the factorial of n, i.e. the product of all the integers between 1 and n, and $0! = 1$. For any finite

E-mail address: sahongnk@gmail.com.

http://dx.doi.org/10.1016/j.crma.2016.06.001
1631-073X/

set S of integers, we denote the greatest common divisor of all the elements of S by $\gcd(S)$. For any prime p, by $\nu_p(n)$ we denote the largest nonnegative integer e such that p^e divides n, and $\nu_p(n)$ is called the normalized *p-adic valuation* of n. Ram [5] proved that the integer $\gcd(\{\binom{n}{k} : 1 \le k \le n-1\})$ equals p if n is a positive power of p, and is equal to 1 otherwise. This result was later strengthened by Joris, Oestreicher and Steinig in [3]. On the other hand, Mendelsohn et al. [4] showed the following elegant identity:

$$\gcd(\left\{\binom{2n}{1}, \binom{2n}{3}, \ldots, \binom{2n}{2n-1}\right\}) = 2^{1+\nu_2(n)}. \tag{1.1}$$

Albree [1] generalized the identity (1.1) by showing that if p is a prime, then

$$\gcd(\left\{\binom{pn}{k} : 1 \le k \le pn, p \not| k\right\}) = p^{1+\nu_p(n)}. \tag{1.2}$$

Our main goal in this paper is to extend (1.2) from the prime number p case to the general composite number case. Let m be a positive integer. An explicit formula for the greatest common divisor of the sequence of the binomial coefficients $\binom{mn}{k}$, where k runs over all the integers between 1 and mn which are coprime to m, is given in this paper. That is, our main result is the following:

Theorem 1.1. *Let m and n be positive integers. Then*

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

The method of the proof of Theorem 1.1 is p-adic in character. Furthermore, we have the following interesting corollaries.

Corollary 1.2. *Let r and n be positive integers. If $p_1, \ldots, p_r$ are r distinct prime numbers, then*

$$\gcd(\left\{\binom{p_1 \ldots p_r n}{k} : 1 \le k \le p_1 \ldots p_r n, \gcd(k, p_1 \ldots p_r) = 1\right\}) = p_1^{1+\nu_{p_1}(n)} \ldots p_r^{1+\nu_{p_r}(n)}.$$

Corollary 1.3. *Let m and n be two relatively prime positive integers. Then*

$$\gcd(\left\{\binom{mn}{k} : 1 \le k \le mn, \gcd(k,m) = 1\right\}) = m.$$

Evidently, if one picks $r = 1$, then Corollary 1.2 becomes Albree's identity (1.2). This paper is organized as follows. In Section 2, we will show several preliminary lemmas. Then we use these lemmas to show Theorem 1.1 in Section 3. In the final section, we propose two interesting open problems.

2. Preliminary lemmas

In this section, we prove three lemmas that are needed in the proof of Theorem 1.1. We begin with the following result, which is Theorem 1.1 when $n = 1$.

Lemma 2.1. *Let n be a positive integer. Then*

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

Proof. Let $G_n = \{\binom{n}{k} : 1 \le k \le n, \gcd(k,n) = 1\}$. Then $n \in G_n$ and so one has $\gcd(G_n) | n$. Let k be an integer with $1 \le k \le n$ and $\gcd(k,n) = 1$. Then we have

$$k\binom{n}{k} = k\frac{n!}{k!(n-k)!} = n\frac{(n-1)!}{(k-1)!(n-k)!} = n\binom{n-1}{k-1}.$$

Thus n divides the integer $k\binom{n}{k}$. But n is coprime to k. It follows that n divides $\binom{n}{k}$. So one has $n | \gcd(G_n)$ and the desired result $\gcd(G_n) = n$ follows immediately. The proof of Lemma 2.1 is complete. □

In the sequel, we investigate the p-adic valuations of the binomial coefficients. Let us recall the so-called Legendre formula on the p-adic valuations of factorials.

Lemma 2.2. *[2] Let n be an integer and let p be a prime number. Then*

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

where $\sigma_p(n)$ stands for the sum of the standard base-p digits of n. Namely, one has $\sigma_p(n) := \sum_{i=0}^{r} a_i$ if $n = \sum_{i=0}^{r} a_i p^i$ with r and a_i being integers such that $r \geq 0$, $a_r > 0$ and $0 \leq a_i \leq p-1$ for all integers i with $0 \leq i \leq r$.

Lemma 2.3. *Let p be a prime number and let $n \geq 1$ and $e \geq 0$ be integers such that $e \leq \nu_p(n)$. Then*

$$\nu_p\left(\binom{n}{p^e}\right) = \nu_p(n) - e.$$

Proof. First let $p \nmid n$. Then $\nu_p(n) = 0$. Since $0 \leq e \leq \nu_p(n)$, one has $e = 0$. It follows that

$$\nu_p\left(\binom{n}{p^e}\right) = \nu_p\left(\binom{n}{1}\right) = \nu_p(n) = 0$$

as desired.

In what follows, we assume that $p|n$. Then $\nu_p(n) \geq 1$. Let $n = p^{\nu_p(n)}\bar{n}$ with $p \nmid \bar{n}$. Write $\bar{n} = \sum_{i=0}^{r} n_i p^i$, where $r \geq 0$ is an integer and $0 \leq n_i \leq p-1$ for all integers i with $0 \leq i \leq r$, $p \nmid n_0$ and $n_r \neq 0$. Then $\sigma_p(n) = \sum_{i=0}^{r} n_i$. Since $p \nmid n_0$, one has $n_0 \geq 1$. But $e \leq \nu_p(n)$. One then deduces that

$$\begin{aligned} n - p^e &= \sum_{i=0}^{r} n_i p^{i+\nu_p(n)} - p^e \\ &= (p^{\nu_p(n)} - p^e) + (n_0 - 1)p^{\nu_p(n)} + \sum_{i=1}^{r} n_i p^{i+\nu_p(n)} \\ &= \sum_{i=e}^{\nu_p(n)-1} (p-1)p^i + (n_0 - 1)p^{\nu_p(n)} + \sum_{i=1}^{r} n_i p^{i+\nu_p(n)}. \end{aligned} \tag{2.1}$$

The right-hand side of (2.1) is the p-adic representation of $n - p^e$. It then follows that

$$\begin{aligned} \sigma_p(n - p^e) &= (p-1)(\nu_p(n) - 1 - (e-1)) + n_0 - 1 + \sum_{i=1}^{r} n_i \\ &= (p-1)(\nu_p(n) - e) - 1 + \sum_{i=0}^{r} n_i \\ &= (p-1)(\nu_p(n) - e) - 1 + \sigma_p(n). \end{aligned}$$

In other words, we have

$$\sigma_p(n - p^e) - \sigma_p(n) = (p-1)(\nu_p(n) - e) - 1. \tag{2.2}$$

So by Lemma 2.2 together with (2.2), one gets that

$$\begin{aligned} \nu_p\left(\binom{n}{p^e}\right) &= \frac{\sigma_p(p^e) + \sigma_p(n - p^e) - \sigma_p(n)}{p-1} \\ &= \frac{1 + (p-1)(\nu_p(n) - e) - 1}{p-1} \\ &= \nu_p(n) - e \end{aligned}$$

as required. So Lemma 2.3 is proved. □

Lemma 2.4. *Let m, n and k be positive integers such that $k \leq mn$ and k is coprime to m. Then for any prime divisor p of m, we have*

$$\nu_p\left(\binom{mn}{k}\right) \geq \nu_p(m) + \nu_p(n).$$

Proof. First of all, one has

$$k\binom{mn}{k} = mn\binom{mn-1}{k-1}. \tag{2.3}$$

Now let p be a prime divisor of m. Then $p^{\nu_p(m)+\nu_p(n)}$ divides the right-hand side of (2.3), which implies that

$$p^{\nu_p(m)+\nu_p(n)} \Big| k\binom{mn}{k}. \tag{2.4}$$

But k is coprime to m and $p|m$. So k is coprime to p, which implies that $\gcd(p^{\nu_p(m)+\nu_p(n)}, k) = 1$. It then follows from (2.4) that $p^{\nu_p(m)+\nu_p(n)}$ divides the binomial coefficient $\binom{mn}{k}$. Hence the desired result follows immediately. This ends the proof of Lemma 2.4. □

3. Proof of Theorem 1.1

We are now in a position to give the proof of Theorem 1.1.

Proof of Theorem 1.1. Let

$$G_{mn} = \left\{ \binom{mn}{k} : 1 \le k \le mn, \gcd(k, m) = 1 \right\}.$$

If $m = 1$, then $1 \in G_{mn}$ and so $\gcd(G_{mn}) = 1$ as desired. If $n = 1$, then by Lemma 2.1, one has $\gcd(G_{mn}) = m$ as required. In the following, we let $m \ge 2$ and $n \ge 2$.

First we let $n|m$. Then $\gcd(m, n) = n$ and

$$G_{mn} = \left\{ \binom{mn}{k} : 1 \le k \le mn, \gcd(k, mn) = 1 \right\}.$$

Hence Lemma 2.1 applied to mn gives us that

$$\gcd(G_{mn}) = mn = m \prod_{\text{prime } p|n} p^{\nu_p(n)} = m \prod_{\text{prime } p|\gcd(m,n)} p^{\nu_p(n)}$$

as desired. Namely, Theorem 1.1 is true if $n|m$.

Consequently, we let $n \nmid m$. Since $\binom{mn}{1} = mn$ is one term of G_{mn}, it follows that $\gcd(G_{mn})$ divides mn. So one needs only to compute the p-adic valuation $\nu_p(\gcd(G_{mn}))$ for all prime divisors p of mn, which will be done in the following. Let p be a prime number such that $p|mn$. Then one has either $p|m$ or $p|n$. We divide the computation of $\nu_p(\gcd(G_{mn}))$ into the following two cases.

Case 1. $p|n$ and $p \nmid m$. Then $\gcd(p^{\nu_p(n)}, m) = 1$ and $1 < p^{\nu_p(n)} \le n < mn$ since $m \ge 2$ and $p \ge 2$ and $p|n$ implying that $\nu_p(n) > 0$. This implies that $\binom{mn}{p^{\nu_p(n)}}$ is one term of G_{mn}. On the other hand, one has $\nu_p(mn) = \nu_p(n)$ since $p \nmid m$. Thus with n replaced by mn and e replaced by $\nu_p(mn)$ in Lemma 2.3, we obtain that

$$\nu_p\left(\binom{mn}{p^{\nu_p(n)}}\right) = \nu_p\left(\binom{mn}{p^{\nu_p(mn)}}\right) = 0.$$

One can then deduce that

$$\nu_p(\gcd(G_{mn})) = \min\left\{ \nu_p\left(\binom{mn}{k}\right) : 1 \le k \le mn, \gcd(k, m) = 1 \right\} = 0. \tag{3.1}$$

Case 2. $p|m$. For all integers k with $1 \le k \le mn$ and $\gcd(k, m) = 1$, by Lemma 2.4 one gets that

$$\nu_p\left(\binom{mn}{k}\right) \ge \nu_p(m) + \nu_p(n). \tag{3.2}$$

Notice that

$$\nu_p\left(\binom{mn}{1}\right) = \nu_p(m) + \nu_p(n). \tag{3.3}$$

It then follows from (3.2) and (3.3) that

$$\min\left\{ \nu_p\left(\binom{mn}{k}\right) : 1 \le k \le mn, \gcd(k, m) = 1 \right\} = \nu_p(m) + \nu_p(n).$$

That is, one has

$$\nu_p(\gcd(G_{mn})) = \nu_p(m) + \nu_p(n). \tag{3.4}$$

Finally, from (3.1) together with (3.4) we derive that

$$\begin{aligned}
\gcd(G_{mn}) &= \prod_{\text{prime } p \mid \gcd(G_{mn})} p^{\nu_p(\gcd(G_{mn}))} \\
&= \prod_{\text{prime } p \mid mn} p^{\nu_p(\gcd(G_{mn}))} \\
&= \Big(\prod_{\text{prime } p \mid m} p^{\nu_p(\gcd(G_{mn}))} \Big) \Big(\prod_{\text{prime } p \mid n, p \nmid m} p^{\nu_p(\gcd(G_{mn}))} \Big) \\
&= \Big(\prod_{\text{prime } p \mid m} p^{\nu_p(m)+\nu_p(n)} \Big) \Big(\prod_{\text{prime } p \mid n, p \nmid m} p^{0} \Big) \\
&= \prod_{\text{prime } p \mid m} p^{\nu_p(m)+\nu_p(n)} \\
&= \Big(\prod_{\text{prime } p \mid m} p^{\nu_p(m)} \Big) \Big(\prod_{\text{prime } p \mid m} p^{\nu_p(n)} \Big) \\
&= m \prod_{\text{prime } p \mid m} p^{\nu_p(n)} = m \prod_{\text{prime } p \mid \gcd(m,n)} p^{\nu_p(n)}
\end{aligned}$$

as required. This concludes the proof of Theorem 1.1. □

4. Concluding remarks

Let $n \geq 2$ be an integer. Then by Ram's theorem [5], we know that

$$\gcd\left(\left\{\binom{n}{k} : 1 \leq k \leq n-1\right\}\right) = \begin{cases} p, & \text{if } n \text{ is a power of } p, \\ 1, & \text{otherwise.} \end{cases}$$

On the other hand, Lemma 2.1 tells us that

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

The following interesting question arises naturally:

Problem 4.1. *Let $n \geq 2$ be an integer. Find an explicit formula for*

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

As in Soulé's interesting paper [6], in what follows we denote by $b(n)$ the smallest nonnegative integer b such that the set of the binomial coefficients $\binom{n}{k}$, where k is an integer with $b < k < n-b$, has a nontrivial common divisor. Granville found that the integer $b(n)$ is the smallest integer of the form $n - p^e$, where p^e is a prime power less or equal to n (see Theorem 3 of [6]). Furthermore, one may ask the following interesting question.

Problem 4.2. *Let $n \geq 2$ be an integer and $b(n)$ be defined as above. Find the explicit formula for*

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

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

and

$$\gcd\left(\left\{\binom{n}{k} : b(n) < k < n - b(n), \gcd(k,n) > 1\right\}\right),$$

respectively.

Acknowledgement

The author would like to thank the anonymous referee for helpful comments, and particularly for having drawn his attention to Soulé's interesting paper [6].

References

[1] J. Albree, The gcd of certain binomial coefficients, Math. Mag. 45 (1972) 259–261.
[2] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Grad. Texts Math., vol. 84, Springer-Verlag, New York, 1990.
[3] H. Joris, C. Oestreicher, J. Steinig, The greatest common divisor of certain sets of binomial coefficients, J. Number Theory 21 (1985) 101–119.
[4] N.S. Mendelsohn, St. Olaf College, Students, divisors of binomial coefficients, Amer. Math. Mon. 78 (1971) 201–202.
[5] B. Ram, Common factors of $n!/m!(n-m)!$ $(m=1,2,\ldots,n-1)$, J. Indian Math. Club (Madras) 1 (1909) 39–43.
[6] C. Soulé, Secant varieties and successive minima, J. Algebraic Geom. 13 (2004) 323–341.