Journal of Number Theory 183 (2018) 428–441

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Some divisibility properties of binomial coefficients

Daniel Yaqubi, Madjid Mirzavaziri *

Department of Pure Mathematics, Ferdowsi University of Mashhad,
P.O. Box 1159, Mashhad 91775, Iran

ARTICLE INFO

Article history:
Received 14 July 2016
Received in revised form 19 August 2017
Accepted 19 August 2017
Available online 20 September 2017
Communicated by the Principal Editors

MSC:
primary 11B65
secondary 05A10

Keywords:
Binomial coefficients
p-adic valuation
Lucas' theorem
Euler's totient theorem
Bernoulli numbers

ABSTRACT

In this paper, we aim to give full or partial proofs for the following three conjectures of V. J. W. Guo and C. Krattenthaler: (1) Let $a > b$ be positive integers, α, β be any integers and p be a prime satisfying $\gcd(p, a) = 1$. Then there exist infinitely many positive integers n for which $\binom{an+\alpha}{bn+\beta} \equiv r \pmod{p}$ for all integers r; (2) For any odd prime p, there are no positive integers $a > b$ such that $\binom{an}{bn} \equiv 0 \pmod{pn-1}$ for all $n \geq 1$; (3) For any positive integer m, there exist positive integers a and b such that $am > b$ and $\binom{amn}{bn} \equiv 0 \pmod{an-1}$ for all $n \geq 1$.

1. Introduction

Binomial coefficients constitute an important class of numbers that arise naturally in mathematics, namely as coefficients in the expansion of the polynomial $(x + y)^n$. Accordingly, they appear in various mathematical areas. An elementary property of

[*] Corresponding author.
E-mail addresses: daniel_yaqubi@yahoo.es (D. Yaqubi), mirzavaziri@um.ac.ir (M. Mirzavaziri).

http://dx.doi.org/10.1016/j.jnt.2017.08.005
0022-314X/© 2017 Published by Elsevier Inc.

binomial coefficients is that $\binom{n}{m}$ is divisible by a prime p for all $1 < m < n$ if and only if n is a power of p. A much more technical result due to Lucas asserts that

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\cdots\binom{n_k}{m_k} \pmod{p},$$

in which $n = n_0+n_1p+\cdots+n_kp^k$ and $m = m_0+m_1p+\cdots+m_kp^k$ are the p-adic expansions of the non-negative integers n and m, respectively. We note that $0 \leq m_i, n_i < p$, for all $i = 0, \ldots, k$. In 1819, Babbage [1] revealed the following congruences for all odd prime p:

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}.$$

In 1862, Wolstenholme [6] strengthened the identity of Babbage by showing that the same congruence holds modulo p^3 for all primes $p \geq 5$. This identity was further generalized by Ljunggren in 1952 to $\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3}$ and even more to $\binom{np}{mp}/\binom{n}{m} \equiv 1 \pmod{p^q}$ by Jacobsthal for all positive integers $n > m$ and primes $p \geq 5$, in which p^q is any power of p dividing $p^3mn(n-m)$. Arithmetic properties of binomial coefficients are studied extensively in the literature and we may refer the interested reader to [6] for an account of Wolstenholme's theorem. Recently, Guo and Krattenthaler [2] studied a similar problem and proved the following conjecture of Sun [4].

Theorem 1.1. *Let a and b be positive integers. If $bn+1$ divides $\binom{an+bn}{an}$ for all sufficiently large positive integers n, then each prime factor of a divides b. In other words, if a has a prime factor not dividing b, then there are infinitely many positive integers n for which $bn+1$ does not divide $\binom{an+bn}{an}$.*

They also stated several conjectures among which are the followings. We aim to prove or give partial proofs to these conjectures.

In Section 2, we prove Conjecture 1.2 in special cases, see Theorems 2.1 and 2.2.

Conjecture 1.2 *([2, Conjecture 7.2]). For any odd prime p, there are no positive integers $a > b$ such that*

$$\binom{an}{bn} \equiv 0 \pmod{pn-1}$$

for all $n \geq 1$.

In Section 3, using only properties of the p-adic valuation, we give a full proof for Conjecture 7.3 of [2].

Conjecture 1.3 *([2, Conjecture 7.3]). For any positive integer m, there exist positive integers a and b such that $am > b$ and*

$$\binom{amn}{bn} \equiv 0 \pmod{an-1}$$

for all $n \geq 1$.

Maxim Vsemirnov [5] has proved that Conjecture 1.4 is not true for $p = 5$. In Section 4, we prove this conjecture in a special case. The conjecture is still open for the cases $p \neq 5$.

Conjecture 1.4 *([2, Conjecture 7.1]). Let $a > b$ be positive integers, α, β be any integers and p be a prime satisfying $\gcd(p, a) = 1$. Then there exist infinitely many positive integers n for which*

$$\binom{an+\alpha}{bn+\beta} \equiv r \pmod{p}$$

for all integers r.

2. Conjecture 1.2

Our first result is the proof of Conjecture 1.2 in the case where $a, b \not\equiv 0 \pmod{p}$. Furthermore, we also provide a partial proof of Conjecture 1.2 in the case where $a \equiv 0 \pmod{p}$; see Theorem 2.2.

Theorem 2.1. *There are no positive integers $a > b$ with $\gcd(ab, p) = 1$ such that*

$$\binom{an}{bn} \equiv 0 \pmod{pn-1}$$

for all $n \geqslant 1$.

Proof. Suppose on the contrary that $a > b$ exist satisfying the conditions of the theorem. Let $1 \leqslant s \leqslant p-1$ be such that $sb \equiv 1 \pmod{p}$, and write

$$\begin{aligned} sa &= pQ + r, \quad (1 \leqslant r \leqslant p-1) \\ sb &= pQ' + 1. \end{aligned}$$

Also, choose $t > 0$ such that $st \equiv -1 \pmod{p}$, and suppose $st = kp - 1$ for some $k \geq 0$. We claim that

$$(pn+t)(p+s) = pK - 1 \Big| \binom{aK}{bK},$$

where $K = pn + ns + t + k$. By Dirichlet's theorem, there are infinitely many primes of the form $pn + t$. If $pn + t$ is prime, Lucas' theorem implies that

$$\begin{aligned}\binom{aK}{bK} &= \binom{a(pn+ns+t+k)}{b(pn+ns+t+k)}\\ &= \binom{a(pn+t)+a(ns+k)}{b(pn+t)+b(ns+k)}\\ &= \binom{a(pn+t)+Q(pn+t)+rn+ak-Qt}{b(pn+t)+Q'(pn+t)+n+bk-Q't}\\ &\equiv \binom{a+Q}{b+Q'}\binom{rn+ak-Qt}{n+bk-Q't} \pmod{pn+t},\end{aligned}$$

since for sufficiently large n we have $rn+ak-Qt, n+bk-Q't < pn+t$. Now we have

$$\begin{aligned}s(n+bk-Q't) &= sn+(pQ'+1)k-Q'(pk-1)\\ &= sn+k+Q'\\ &\leqslant srn+rk+Q\\ &\leqslant srn+(pQ+r)k-Q(pk-1) = s(rn+ak-Qt)\end{aligned}$$

whence $\binom{rn+ak-Qt}{n+bk-Q't} \neq 0$. The proof is complete. □

Notice that Conjecture 1.2 is still open in the cases where $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$. In the next theorem, we consider the case where $a = cp$ and $b = pk + r$ $(1 \leqslant r \leqslant p-1)$ and give a partial answer to Conjecture 1.2 in this case.

We know that for each prime p and $\varepsilon > 0$ there is a real number $M_p(\varepsilon)$ such that for each $x \geqslant M_p(\varepsilon)$ there is a prime number q in the interval $(x, (1+\varepsilon)x)$ with $q \equiv -1 \pmod p$ [3]. Moreover, there is a real number $M'_p(\varepsilon)$ such that for each $x \geqslant M'_p(\varepsilon)$ there are at least two prime numbers q, q' in the interval $(x, (1+\varepsilon)x)$ with $q, q' \equiv -1 \pmod p$.

In the following we may assume $b < c(p-r)$, since if $b \geqslant c(p-r)$ then $\binom{pcn}{bn} = \binom{pcn}{b'n}$, where $b' = pc - b$. We have $b' = pk' + r'$, where $k' = c-k-1$, $r' = p-r$, and $b' < c(p-r')$.

Theorem 2.2. *Let p be an odd prime, $1 \leqslant r \leqslant p-1$, and $\gamma = \frac{p^2r+p^2+r^2-pr}{p^2(p+1)}$.*

(i) *If $pk+r \leqslant cp(1-\gamma)$, then there are no positive integers $c \geqslant M_p(\frac{(p-r)^2}{pr(p+1)})$ and k such that*

$$\binom{pcn}{(pk+r)n} \equiv 0 \pmod{pn-1},$$

for all $n \geqslant 1$.

(ii) *If $cp(1-\gamma) < pk+r < c(p-r)$ and $r \leqslant \frac{p-3}{2}$, then there are no positive integers $k \geqslant 2M'_p(\frac{p-(2r+1)}{p+1})$ and c such that*

$$\binom{pcn}{(pk+r)n} \equiv 0 \pmod{pn-1},$$

for all $n \geqslant 1$.

Proof. (i) Put $b = pk + r$. We have $-\frac{b}{c} \geqslant (\gamma - 1)p$. Thus

$$\frac{\frac{p(c-k)}{r} - 1}{c} = \frac{p(c-k) - r}{rc} = \frac{p}{r} - \frac{b}{rc} \geqslant \frac{p}{r} + \frac{\gamma p}{r} - \frac{p}{r} = 1 + \frac{(p-r)^2}{pr(p+1)} > 1.$$

Now since $c \geqslant M_p(\frac{(p-r)^2}{pr(p+1)})$, there is a prime number $pn - 1$ with

$$c < pn - 1 < \frac{p(c-k)}{r} - 1.$$

This gives the result, since $k \leqslant rn + k \leqslant c < pn - 1$ and Lucas's theorem implies

$$\binom{pcn}{(pk+r)n} = \binom{c(pn-1)+c}{k(pn-1)+rn+k} \equiv \binom{c}{k}\binom{c}{rn+k} \pmod{pn-1}.$$

(ii) For $\alpha = \frac{p+1}{2(p-r)}$ we have

$$\frac{k}{\alpha k} = \frac{2(p-r)}{p+1} = 1 + \frac{p-(2r+1)}{p+1} > 1$$

and since $\alpha k \geqslant M'_p(\frac{p-(2r+1)}{p+1})$, there are two prime numbers $pm - 1$, $pn - 1$ with $\alpha k < pm - 1 < pn - 1 < k$. We have

$$k = \frac{b-r}{p} < \frac{c(p-r)-r}{p} = c - \frac{r(c+1)}{p} < c.$$

Furthermore,

$$rn + k < r \cdot \frac{k+1}{p} + k = \frac{rk+b}{p} < \frac{rk + c(p-r)}{p} < \frac{rc + c(p-r)}{p} = c.$$

Moreover,

$$\frac{c}{k} < \frac{b}{k(1-\gamma)p} = \frac{kp+r}{kp \cdot \frac{(p^2+r)(p-r)}{p^2(p+1)}} \leqslant \frac{p+1}{p-r},$$

where the last inequality is true since $k \geqslant p$. We can therefore deduce that

$$pn - 1 < k < c < 2 \cdot \frac{\frac{p+1}{p-r}}{2} k = 2\alpha k < 2(pm-1).$$

We have $c+1 \leqslant 2(pm-1) < 2(pn-1)$. Write $c = (pn-1)+R$ and $rn+k = (pn-1)+R'$. We know that $pn - 1 > R > R'$. Now Lucas' theorem implies

$$\binom{pcn}{(pk+r)n} = \binom{c(pn-1)+(pn-1)+R}{k(pn-1)+(pn-1)+R'} \equiv \binom{c+1}{k+1}\binom{R}{R'} \pmod{pn-1}.$$

The latter is not congruent to 0, since

$$\lfloor\frac{c+1}{pn-1}\rfloor - \lfloor\frac{k+1}{pn-1}\rfloor - \lfloor\frac{c-k}{pn-1}\rfloor \leqslant 1-1-0=0. \qquad \square$$

Lemma 2.3. *Let p be an odd prime, $1 \leqslant r \leqslant p-2$, $j = \lfloor\frac{p}{p-r}\rfloor$, and $\alpha = \frac{p}{(p-r)(j+1)}$. Then there is an $0 < \varepsilon(p,r) < 1$ with*

$$\alpha < \frac{p+\varepsilon(p,r)}{(p-r)(j+1)} < \frac{\frac{r}{p-r}}{j-1+\frac{r}{p}}.$$

Proof. A simple verification shows that

$$\alpha < \frac{\frac{r}{p-r}}{j-1+\frac{r}{p}}$$

if and only if $p-r \nmid p$ or equivalently $r \neq p-1$. This implies the existence of $\varepsilon(p,r)$. $\square$

On the other hand, we let $c = j(pn-1)+R$, $0 \leqslant R \leqslant pn-2$, $rn+k = (pn-1)+R'$ with $0 \leqslant R' \leqslant pn-2$, and suppose $pn-1 = \theta k$, where $\alpha < \theta < \beta$. Then by Lemma 2.3,

$$\begin{aligned} R' + j\theta k &= k-(pn-1)+rn+j\theta k \\ &= k-\theta k + r\cdot\frac{\theta k+1}{p} + j\theta k \\ &= k(1+(-1+\frac{r}{p}+j)\theta)+\frac{r}{p} \\ &\leqslant k(1+(-1+\frac{r}{p}+j)\beta)+\frac{r}{p} \\ &= k(1+(j-1+\frac{r}{p})\beta)+\frac{r}{p} \\ &< k(1+\frac{r}{p-r})+\frac{r}{p} \\ &< \frac{p}{p-r}k+\frac{r}{p-r} \\ &< c. \end{aligned}$$

Hence

$$R = c-j(pn-1) = c-j\theta k > R'.$$

This shows that

$$\lfloor\frac{c}{pn-1}\rfloor - \lfloor\frac{rn+k}{pn-1}\rfloor - \lfloor\frac{c-(rn+k)}{pn-1}\rfloor = j-1-(j-1+\lfloor\frac{R-R'}{pn-1}\rfloor) = 0,$$

from which the result follows.

3. Conjecture 1.3

In this section, using only properties of the p-adic valuation, we give an inductive proof of Conjecture 7.3 of [2]. For $n \in \mathbb{N}$ and a prime p, the p-adic valuation of n, denoted by $\nu_p(n)$ is the highest power of p that divides n. The expansion of $n \in \mathbb{N}$ in base p is written as $n = n_0 + n_1 p + \ldots + n_k p^k$ with integers $0 \leqslant n_i \leqslant p-1$ and $n_k \neq 0$. *Legendre's classical formula* for the factorials $\nu_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$ appears in elementary textbooks.

Theorem 3.1. *For any positive integer m, there are positive integers a and b such that $am > b$ and*

$$\binom{amn}{bn} \equiv 0 \pmod{an-1}$$

for all $n \geqslant 1$.

Proof. Let $p_1 = 2 < p_2 = 3 < p_3 = 5 < \cdots$ be the sequence of prime numbers. Choose t such that $p_t > 3m$ and put

$$a = 6p_3 \ldots p_t,$$
$$b = 4p_3 \ldots p_t.$$

Let n be a positive integer and $q^\alpha \mid an-1$ for some prime number q. We aim at showing that $q^\alpha \mid \binom{amn}{bn}$. This of course proves that $an-1 \mid \binom{amn}{bn}$.

Write bn in base q in the form $\sum_{j=0}^{N} r_j q^j$, where $N = \alpha - 1$ or α since $bn \geqslant q^{\alpha-1}$. First we show that $m < r_0$. We have

$$r_0 \equiv bn = 4p_3 \ldots p_t n \equiv 2 \cdot 3^* \cdot 6p_3 \ldots p_t n = 2 \cdot 3^* an \equiv 2 \cdot 3^* \pmod{q},$$

where 3^* is the inverse of 3 mod q. We know that

$$3^* = \begin{cases} \frac{q+1}{3}, & \text{if } 3 \mid q+1, \\ \frac{2q+1}{3}, & \text{if } 3 \mid q+2. \end{cases}$$

Note that 3^* exists since $q \neq 3$. We thus have

$$r_0 = 2 \cdot 3^* = \begin{cases} 2 \cdot \frac{q+1}{3} > \frac{q}{3}, & \text{if } 3 \mid q+1, \\ 2 \cdot \frac{2q+1}{3} - q = \frac{q+2}{3} > \frac{q}{3}, & \text{if } 3 \mid q+2. \end{cases}$$

We have $\gcd(q, p_1 p_2 \ldots p_t) = 1$. Hence $q > p_t > 3m$. This shows that $m < r_0$. We therefore have

$$\lfloor\frac{bn-m}{q^i}\rfloor = \lfloor\frac{\sum_{j=0}^{N} r_j q^j - m}{q^i}\rfloor = \lfloor\sum_{j=i}^{N} r_j q^{j-i} + \frac{\sum_{j=1}^{i-1} r_j q^j + r_0 - m}{q^i}\rfloor$$
$$= \sum_{j=i}^{N} r_j q^{j-i} = \lfloor\frac{bn}{q^i}\rfloor.$$

Now let $an-1=kq^\alpha$, where $\gcd(k,q)=1$. We evaluate the q-adic valuation $v_q(\binom{amn}{bn})$. If $N=\alpha$ then

$$\begin{aligned} v_q(\binom{amn}{bn}) &\geqslant \sum_{i=1}^{\alpha}\big(\lfloor\frac{amn}{q^i}\rfloor - \lfloor\frac{bn}{q^i}\rfloor - \lfloor\frac{(am-b)n}{q^i}\rfloor\big) \\ &\geqslant \sum_{i=1}^{\alpha}\big(mkq^{\alpha-i} - \lfloor\frac{bn}{q^i}\rfloor - \lfloor\frac{(am-b)n}{q^i}\rfloor\big) \\ &= \sum_{i=1}^{\alpha}\big(mkq^{\alpha-i} - \lfloor\frac{bn}{q^i}\rfloor - \lfloor\frac{mkq^\alpha + m - bn}{q^i}\rfloor\big) \\ &= \sum_{i=1}^{\alpha}\big(mkq^{\alpha-i} - \lfloor\frac{bn}{q^i}\rfloor - mkq^{\alpha-i} - \lfloor\frac{m-bn}{q^i}\rfloor\big) \\ &= \sum_{i=1}^{\alpha}\big(-\lfloor\frac{bn}{q^i}\rfloor - \lfloor-\frac{bn-m}{q^i}\rfloor\big) \\ &= \sum_{i=1}^{\alpha}\big(-\lfloor\frac{bn}{q^i}\rfloor + \lfloor\frac{bn-m}{q^i}\rfloor + 1\big) \\ &= \sum_{i=1}^{\alpha} 1 = \alpha, \end{aligned}$$

since $\frac{bn-m}{q^i}$ is not an integer.

On the other hand, if $N=\alpha-1$ then

$$\begin{aligned} v_q(\binom{amn}{bn}) &= mk + \sum_{i=1}^{\alpha-1}\big(\lfloor\frac{amn}{q^i}\rfloor - \lfloor\frac{bn}{q^i}\rfloor - \lfloor\frac{(am-b)n}{q^i}\rfloor\big) \\ &\geqslant mk + \alpha - 1 \geqslant \alpha. \end{aligned}$$

Thus $q^\alpha \mid \binom{amn}{bn}$. □

4. Conjecture 1.4

Maxim Vsemirnov [5] proved that Conjecture 1.4 is not true for $p=5$. Namely, he proved the following theorem.

Theorem 4.1. *Let $p = 5$, $a = 4$, $b = 2$. If $(\alpha, \beta) \in \{(0,0), (1,0), (1,1)\}$, then*

$$\binom{4n+\alpha}{2n+\beta} \equiv 0, 1 \ \ \textit{or} \ \ 4 \pmod 5.$$

Also, if $(\alpha, \beta) \in \{(2,1), (3,1), (3,2)\}$, then

$$\binom{4n+\alpha}{2n+\beta} \equiv 0, 2 \ \ \textit{or} \ \ 3 \pmod 5.$$

In the following, we prove Conjecture 1.4 in a special case. We know that if $\gcd(x, y) = 1$, then there is an integer $1 \leqslant x' \leqslant y - 1$ with $y \mid xx' - 1$. We denote this x' by $\mathrm{Inv}_y(x)$. Moreover, for an integer x we denote the p-adic valuation of x by $v_p(x)$.

Theorem 4.2. *Let a and b be positive integers with $a > b$, let α and β be integers, and let $d = \gcd(a, b)$, $c = \frac{a}{d}$, $e = \gcd(p - 1, a)$. Furthermore, let p be a prime such that $p > a + 2b$. Then*

(i) *if $e < c$ or $v_2(a) \leqslant v_2(p - 1)$, then for each $r = 0, 1, \ldots, p - 1$, there are infinitely many positive integers n such that*

$$\binom{an+\alpha}{bn+\beta} \equiv r \pmod p;$$

(ii) *if $e \geqslant c$ and $v_2(a) > v_2(p - 1)$, then for each*

$$r \notin \{(2\mu-1)e + p + \alpha - 2 + r' : 0 \leqslant r' \leqslant e - c, \lceil \frac{e+2-p-\alpha}{2e} \rceil \leqslant \mu \leqslant \lceil \frac{c+1-\alpha}{2e} \rceil\},$$

there are infinitely many positive integers n such that

$$\binom{an+\alpha}{bn+\beta} \equiv r \pmod p.$$

Proof. By Euler's totient theorem, we have $p^{\varphi(a)} \equiv 1 \pmod a$, since $\gcd(p, a) = 1$. For an arbitrary positive integer N, put $u = N\varphi(a)$. Thus

$$p^{ui} \equiv 1 \pmod a, \quad i \in \mathbb{N}.$$

In particular, there is an integer m with $p^u - 1 = am$. Thus $m = -\mathrm{Inv}_p(a)$. Put $t = (p - 1) - r$. Write $c - t - \alpha = \mu e + \rho$, where $0 \leqslant \rho \leqslant e - 1$. Note that $e \mid c - t - \alpha - \rho$. Suppose

$$\varepsilon = \begin{cases} 0, & \text{if } \rho \leqslant c - 2, \\ 1, & \text{otherwise.} \end{cases}$$

If $e < c$ then put

$$\begin{aligned}K = {} & \frac{c-t-\alpha-\rho}{e} \cdot \big(p\mathrm{Inv}_{\frac{a}{e}}(\frac{p(p-1)}{e})\big) \\ & +(c-t-\alpha-\rho)am\mathrm{Inv}_p(a+1) - (\beta-1)a^2m\mathrm{Inv}_p(b(a+1)) + Lpa,\end{aligned}$$

where L is sufficiently large so that $K > 1$. Note that $\varepsilon = 0$ in this case, since $\rho \leqslant e-1 \leqslant c-2$.

If $e \geqslant c$ and $v_2(a) \leqslant v_2(p-1)$, then put

$$\begin{aligned}K = {} & \frac{c-t-\alpha-\rho}{e} \cdot \big(p\mathrm{Inv}_{\frac{a}{e}}(\frac{p(p-1)(1+\varepsilon)}{e})\big) \\ & +(c-t-\alpha-\rho)am\mathrm{Inv}_p(a+1) - (\beta-1)a^2m\mathrm{Inv}_p(b(a+1)) + Lpa,\end{aligned}$$

where L is sufficiently large so that $K > 1$. Note that $\mathrm{Inv}_{\frac{a}{e}}(1+\varepsilon)$ exists, since $\frac{a}{e}$ is odd in this case.

Finally, if $e \geqslant c$ and $v_2(a) > v_2(p-1)$, then put

$$\begin{aligned}K = {} & \frac{c-t-\alpha-\rho}{(1+\varepsilon)e} \cdot \big(p\mathrm{Inv}_{\frac{a}{(1+\varepsilon)e}}(\frac{p(p-1)}{e})\big) \\ & +(c-t-\alpha-\rho)am\mathrm{Inv}_p(a+1) - (\beta-1)a^2m\mathrm{Inv}_p(b(a+1)) + Lpa,\end{aligned}$$

where L is sufficiently large so that $K > 1$. Note that $\frac{c-t-\alpha-\rho}{e}$ is even by our assumption on r in this case.

In each of the above cases we have

$$\begin{aligned}K(p-1)(1+\varepsilon) &\equiv c-t-\alpha-\rho \pmod{a}, \\ mb\big(K(p-1)(a+1+\varepsilon) - (c-t-\alpha-\rho)\big) &\equiv \beta - 1 \pmod{p}.\end{aligned}$$

Let

$$M = K(p-1)(d(c-1)+1) - (c-1) + \rho,$$

and

$$\begin{aligned}\mathbb{I}_2 &= \{M - k(c-1) : k = 0, 1, \ldots, K(p-1)(d+\varepsilon) - 1\}, \\ \mathbb{I}_1 &= \{1, 2, \ldots, M\} \setminus \mathbb{I}_2.\end{aligned}$$

We have

$$\begin{aligned}
&p^{u(M+1)} - t - \sum_{i\in\mathbb{I}_1} p^{ui} - \sum_{i\in\mathbb{I}_2} 2p^{ui} - \alpha \\
&\equiv 1 - t - (M - K(p-1)(d+\varepsilon)) - 2K(p-1)(d+\varepsilon) - \alpha \\
&= 1 - t - \alpha - K(p-1)(a+1+\varepsilon) + (c-1) - \rho \\
&\equiv c - t - \alpha - \rho - K(p-1)(1+\varepsilon) \\
&\equiv 0 \pmod{a}.
\end{aligned}$$

Hence, there is a positive integer n such that

$$an + \alpha = p^{u(M+1)} - t - \sum_{i\in\mathbb{I}_1} p^{ui} - \sum_{i\in\mathbb{I}_2} 2p^{ui}.$$

Write $an+\alpha$ in base p as $\sum_{s=0}^{u(M+1)} a_s p^s$. Then we have

$$a_s = \begin{cases} p-1-t, & \text{if } s = 0, \\ p-2, & \text{if } s = ui \text{ for some } i \in \mathbb{I}_1, \\ p-3, & \text{if } s = ui \text{ for some } i \in \mathbb{I}_2, \\ p-1, & \text{otherwise.} \end{cases}$$

We now aim to find digits of $bn+\beta$ in base p. If $bn+\beta = \sum_{s=0}^{u(M+1)} b_s p^s$ then b_s is the remainder of $\lfloor \frac{bn+\beta}{p^s} \rfloor$ mod p. In fact, we need to find b_s for $s = 0, u, 2u, \ldots, Mu$.

We have

$$\begin{aligned}
bn + \beta &= \frac{b}{a}\big(p^{u(M+1)} - t - \sum_{i\in\mathbb{I}_1} p^{ui} - \sum_{i\in\mathbb{I}_2} 2p^{ui}\big) - \frac{b}{a}\alpha + \beta \\
&= \frac{b}{a}\big(p^{u(M+1)} - 1 - \sum_{i\in\mathbb{I}_1} (p^{ui}-1) - \sum_{i\in\mathbb{I}_2} 2(p^{ui}-1)\big) \\
&\quad + \frac{b}{a}(1 - t - (M - K(p-1)(d+\varepsilon)) - 2K(p-1)(d+\varepsilon) - \alpha) + \beta \\
&= \frac{b}{a}\big(p^{u(M+1)} - 1 - \sum_{i\in\mathbb{I}_1} (p^{ui}-1) - \sum_{i\in\mathbb{I}_2} 2(p^{ui}-1)\big) \\
&\quad + \beta - \frac{b}{a}\big(c - t - \alpha - \rho - K(p-1)(a+1+\varepsilon)\big).
\end{aligned}$$

Thus

$$\begin{aligned}
bn + \beta &\equiv -mb\big(p^{u(M+1)} - 1 - \sum_{i\in\mathbb{I}_1} (p^{ui}-1) - \sum_{i\in\mathbb{I}_2} 2(p^{ui}-1)\big) \\
&\quad + \beta - mb\big(K(p-1)(a+1+\varepsilon) - (c - t - \alpha - \rho)\big) \\
&\equiv \beta - (\beta - 1) \equiv 1 \pmod{p}.
\end{aligned}$$

This shows that $b_0 = 1$. Given s, for $j = 1, 2$ let $I_{s,j}$ be the number of $i \in \mathbb{I}_j$ with $i \geqslant s$. For $s \in \mathbb{I}_j$ we have

$$\begin{aligned}
\lfloor \frac{bn+\beta}{p^{us}} \rfloor &= \lfloor \frac{b}{a}\big(p^{u(M+1-s)} - 1 - \sum_{s\leqslant i \in \mathbb{I}_1} (p^{u(i-s)} - 1) - \sum_{s \leqslant i \in \mathbb{I}_2} (2p^{u(i-s)} - 2) \\
&\quad - \sum_{s>i\in\mathbb{I}_1} \frac{1}{p^{u(s-i)}} - \sum_{s>i\in\mathbb{I}_2} \frac{2}{p^{u(s-i)}} - \frac{t}{p^{us}} - I_{s,1} - 2I_{s,2} + 1\big) + \frac{\beta}{p^{us}} \rfloor \\
&= \frac{b}{a}\big(p^{u(M+1-s)} - 1 - \sum_{s\leqslant i \in \mathbb{I}_1} (p^{u(s-i)} - 1) - \sum_{s \leqslant i \in \mathbb{I}_2} (2p^{u(s-i)} - 2)\big) \\
&\quad + \lfloor \frac{b}{a}\big(- \sum_{s>i\in\mathbb{I}_1} \frac{1}{p^{u(s-i)}} - \sum_{s>i\in\mathbb{I}_2} \frac{2}{p^{u(s-i)}} - \frac{t}{p^{us}} - I_{s,1} - 2I_{s,2} + 1\big) + \frac{\beta}{p^{us}} \rfloor \\
&\equiv -mb(-1 + I_{s,1} + 2I_{s,2} - j) - \lfloor \frac{b}{a}(-1 + I_{s,1} + 2I_{s,2}) \rfloor - 1 \pmod{p}.
\end{aligned}$$

Let $I_{s,1} + I_{s,2} - 1 = cq_s + r_s$, where $0 \leqslant r_s < c$. Then for $s \in \mathbb{I}_j$ we have

$$b_{su} = mb(j - r_s) - \lfloor \frac{br_s}{a} \rfloor - 1 \equiv m(a\lfloor \frac{br_s}{a} \rfloor + a - b(r_s - j)) \pmod{p}.$$

Let us evaluate r_s for $s \in \mathbb{I}_j$. If $j = 2$ then $s = M - k(c-1)$ for some $k = 0, 1, \ldots, K(p-1)(d+\varepsilon) - 1$. Thus

$$I_{s,1} = M - (M - k(c-1)) + 1 - (k+1), \quad I_{s,2} = k + 1.$$

So

$$cq_s + r_s = k(c-1) + 1 + (k+1) - 1 \equiv 1 \pmod{c}.$$

Hence $r_s = 1$, whenever $s \in \mathbb{I}_2$. Note that we have $K(p-1)(d+\varepsilon)$ times occurrence of $r_s = 1$.

Moreover, if $j = 1$ then $s = M - k(c-1) - s'$ for some $k = 0, 1, \ldots, K(p-1)(d+\varepsilon) - 1$ and $s' = 1, 2, \ldots, c-2$. Thus

$$I_{s,1} = M - (M - k(c-1) - s') + 1 - (k+1), \quad I_{s,2} = k + 1.$$

So

$$cq_s + r_s = k(c-1) + s' + 1 + (k+1) - 1 \equiv s' + 1 \pmod{c}.$$

Hence $r_s = 2, \ldots, c-1$, whenever $s \in \mathbb{I}_1$. Note that we have $K(p-1)(d+\varepsilon-1)$ times occurrence of $r_s = \rho + 2 - \varepsilon(c-1), \ldots, c-1$ and $K(p-1)(d+\varepsilon)$ times occurrence of $r_s = 2, \ldots, \rho + 1 - \varepsilon(c-1)$.

Now we show that if $s \in \mathbb{I}_1$ then $b_{su}+1 \not\equiv 0 \pmod{p}$ and if $s \in \mathbb{I}_2$ then $b_{su}+1, b_{su}+2 \not\equiv 0 \pmod{p}$.

Let $s \in \mathbb{I}_j$. Then

$$b_{su}+1 \equiv m(a\lfloor\frac{br_s}{a}\rfloor - b(r_s-j)) \pmod{p}.$$

Now if $p \mid b_{su}+1$ then $p \mid a\lfloor\frac{br_s}{a}\rfloor - b(r_s-j)$. The latter holds if and only if $a\lfloor\frac{br_s}{a}\rfloor - b(r_s-j) = 0$, since

$$|b(r_s-j) - a\lfloor\frac{br_s}{a}\rfloor| \leqslant a(\frac{br_s}{a} - \lfloor\frac{br_s}{a}\rfloor) + jb \leqslant a+2b < p$$

Thus we should have $a \mid b(r_s-j)$ which implies that $c \mid r_s - j$. This is a contradiction, since $r_s < c$ and $r_s \neq j$ whenever $s \in \mathbb{I}_j$.

Let $s \in \mathbb{I}_2$. Then

$$b_{su}+2 \equiv m(a\lfloor\frac{br_s}{a}\rfloor - a - b(r_s-2)) \pmod{p}.$$

We know that $r_s = 1$ whenever $s \in \mathbb{I}_2$. Thus if $p \mid b_{su}+2$ then we should have $p \mid a-b$. The latter is impossible since $p > a-b$.

We therefore have

$$\begin{aligned}\binom{an+\alpha}{bn+\beta} &\equiv \binom{p-1-t}{b_0}\prod_{s\in\mathbb{I}_1}(b_{su}+1)\prod_{s\in\mathbb{I}_2}(b_{su}+1)(b_{su}+2)\\ &\equiv -(1+t)\prod_{r_s=2}^{\rho+1-\varepsilon(c-1)}(b_{su}+1)^{K(p-1)(d+\varepsilon)}\prod_{r_s=\rho+2-\varepsilon(c-1)}^{c-1}(b_{su}+1)^{K(p-1)(d+\varepsilon-1)}\\ &\quad\cdot(mb)^{K(p-1)(d+\varepsilon)}(m(b-a))^{K(p-1)(d+\varepsilon)}\\ &\equiv -(1+t)\\ &\equiv -(1+(p-1)-r)\\ &\equiv r \pmod{p}.\end{aligned}$$

Note that there are infinitely many such n, since N was arbitrary. □

Acknowledgments

The authors would like to thank the anonymous referee for her/his careful reading and invaluable suggestions. This paper was written during the first author's sabbatical period in the Department of Mathematics at the University of Vienna. The authors also wish to thank professor Christian Krattenthaler and Mohammad Farrokhi D. G. for some helpful comments.

References

[1] C. Babbage, Demonstration of a theorem relating to prime numbers, Edinb. Philos. J. 1 (1819) 46–49.

[2] V.J.W. Guo, C. Krattenthaler, Some divisibility properties of binomial and q-binomial coefficients, J. Number Theory 135 (2014) 167–189.

[3] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, 6th ed., Oxford University Press, 2008, p. 494.

[4] Z.-W. Sun, On divisibility of binomial coefficients, J. Aust. Math. Soc. 93 (2012) 189–201.

[5] M. Vsemirnov, On a conjecture of Guo and Krattenthaler, Int. J. Number Theory 10 (6) (2014) 1541–1543.

[6] J. Wolstenholme, On certain properties of prime numbers, Q. J. Pure Appl. Math. 5 (1862) 35–39.