J. Number Theory 126(2007), no. 2, 287–296.

CONGRUENCES FOR SUMS OF BINOMIAL COEFFICIENTS

Zhi-Wei Sun[1] and Roberto Tauraso[2]

[1]Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/~zwsun

[2]Dipartimento di Matematica
Università di Roma "Tor Vergata"
Roma 00133, Italy
tauraso@mat.uniroma2.it
http://www.mat.uniroma2.it/∼tauraso

Abstract. Let $q > 1$ and $m > 0$ be relatively prime integers. We find an explicit period $\nu_m(q)$ such that for any integers $n > 0$ and r we have

$$\begin{bmatrix} n+\nu_m(q) \\ r \end{bmatrix}_m (a) \equiv \begin{bmatrix} n \\ r \end{bmatrix}_m (a) \pmod q$$

whenever a is an integer with $\gcd(1-(-a)^m, q) = 1$, or $a \equiv -1 \pmod q$, or $a \equiv 1 \pmod q$ and $2 \mid m$, where $\begin{bmatrix} n \\ r \end{bmatrix}_m (a) = \sum_{k\equiv r \pmod m} \binom{n}{k} a^k$. This is a further extension of a congruence of Glaisher.

1. Introduction and main results

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. Following [S95, S02], for $m \in \mathbb{Z}^+$, $n \in \mathbb{N}$ and $r \in \mathbb{Z}$ we set

$$\begin{bmatrix} n \\ r \end{bmatrix}_m = \sum_{\substack{0\leqslant k\leqslant n \\ k\equiv r \pmod m}} \binom{n}{k} = |\{X \subseteq \{1, \ldots, n\} : |X| \equiv r \pmod m\}| \quad (1.1)$$

and

$$\begin{Bmatrix} n \\ r \end{Bmatrix}_m = \sum_{\substack{0\leqslant k\leqslant n \\ k\equiv r \pmod m}} (-1)^{\frac{k-r}{m}} \binom{n}{k} = \begin{bmatrix} n \\ r \end{bmatrix}_{2m} - \begin{bmatrix} n \\ r+m \end{bmatrix}_{2m}.$$

2000 *Mathematics Subject Classifications.* Primary 11B65; Secondary 05A10, 11A07.

The first author is supported by the National Science Fund for Distinguished Young Scholars (Grant No. 10425103) in China.

Such sums occur in several topics of number theory or combinatorics. (See, e.g., [SS, H, GS, S02].)

Let p be an odd prime. In 1899 J. W. L. Glaisher obtained the following congruence:

$$\begin{bmatrix} n+p-1 \\ r \end{bmatrix}_{p-1} \equiv \begin{bmatrix} n \\ r \end{bmatrix}_{p-1} \pmod p \quad \text{for any } n \in \mathbb{Z}^+ \text{ and } r \in \mathbb{Z}.$$

Since an odd integer is not divisible by $p-1$, this implies Hermite's result that $\left[{n \atop 0}\right]_{p-1} \equiv 1 \pmod p$ for $n = 1, 3, 5, \ldots$ (cf. L. E. Dickson [D, p. 271]). A sophisticated proof of Glaisher's congruence can be found in A. Granville [G97]; the first author observed in 2004 that Glaisher's congruence can be proved immediately by induction on n.

Before stating our further extension of Glaisher's result, let us introduce some notations.

Let $m \in \mathbb{Z}^+$, $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. We set

$$\begin{bmatrix} n \\ r \end{bmatrix}_m (a) = \sum_{\substack{0 \leqslant k \leqslant n \\ k \equiv r \pmod m}} \binom{n}{k} a^k \quad \text{for } a \in \mathbb{Z}. \tag{1.2}$$

Obviously $\left[{n \atop r}\right]_m (1) = \left[{n \atop r}\right]_m$, and

$$\begin{bmatrix} n \\ r \end{bmatrix}_m (-1) = \begin{cases} (-1)^r \left[{n \atop r}\right]_m & \text{if } 2 \mid m, \\ (-1)^r \left\{{n \atop r}\right\}_m & \text{if } 2 \nmid m. \end{cases}$$

It is easy to see that

$$\begin{bmatrix} n+1 \\ r \end{bmatrix}_m (a) = \begin{bmatrix} n \\ r \end{bmatrix}_m (a) + a \begin{bmatrix} n \\ r-1 \end{bmatrix}_m (a). \tag{1.3}$$

Let $a, b \in \mathbb{Z}$ and $q, m, n \in \mathbb{Z}^+$. Clearly

$$\begin{aligned} & (x+a)^n \equiv x^n + b \mod (q, x^m - 1) \\ \iff & \sum_{r=0}^{m-1} \sum_{\substack{0 \leqslant k < n \\ k \equiv r \pmod m}} \binom{n}{k} x^k a^{n-k} \equiv b \mod (q, x^m - 1) \\ \iff & \sum_{\substack{0 \leqslant k < n \\ k \equiv r \pmod m}} \binom{n}{k} a^{n-k} \equiv \begin{cases} b \pmod q & \text{if } r = 0, \\ 0 \pmod q & \text{if } 0 < r < m \end{cases} \\ \iff & \sum_{\substack{1 \leqslant k \leqslant n \\ k \equiv r \pmod m}} \binom{n}{k} a^k \equiv \begin{cases} b \pmod q & \text{if } r \equiv n \pmod m, \\ 0 \pmod q & \text{otherwise.} \end{cases} \end{aligned}$$

(See also [G05].) Now that the congruence condition $(x+a)^n \equiv x^n + a \bmod (n, x^m - 1)$ plays a central role in the polynomial time primality test given by Agrawal, Kayal and Saxena [AKS], it is interesting to investigate periodicity of $\left[{n \atop r}\right]_m(a) \bmod q$ (where $r \in \mathbb{Z}$) with respect to n.

Let $q > 1$ and $m > 0$ be integers with $\gcd(q,m) = 1$, where $\gcd(q,m)$ denotes the greatest common divisor of q and m. Write q in the factorization form $\prod_{s=1}^{t} p_s^{\alpha_s}$ where $p_1, \ldots, p_t$ are distinct primes and $\alpha_1, \ldots, \alpha_t \in \mathbb{Z}^+$. We define

$$\nu_m(q) = \mathrm{lcm}[p_1^{\alpha_1 - 1}(p_1^{\beta_1} - 1), \ldots, p_t^{\alpha_t - 1}(p_t^{\beta_t} - 1)], \tag{1.4}$$

where $\mathrm{lcm}[n_1, \ldots, n_t]$ represents the least common multiple of those $n_s \in \mathbb{Z}^+$ with $1 \leqslant s \leqslant t$, and each β_s is the order of p_s modulo m (i.e., β_s is the smallest positive integer with $p_s^{\beta_s} \equiv 1 \pmod{m}$). Clearly $\nu_1(q) = \mathrm{lcm}[\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_t^{\alpha_t})]$ divides $\varphi(q)$, where φ is Euler's totient function. Since $\varphi(p_s^{\alpha_s}) \mid \nu_m(q)$ for each $s = 1, \ldots, t$, if $a \in \mathbb{Z}$ is relatively prime to q, then by Euler's theorem $a^{\nu_m(q)} \equiv 1 \pmod{p_s^{\alpha_s}}$ and therefore $a^{\nu_m(q)} \equiv 1 \pmod{q}$. Note also that $\nu_{p-1}(p^\alpha) = \varphi(p^\alpha)$ for any prime p and $\alpha \in \mathbb{Z}^+$.

Now we present our first theorem.

Theorem 1.1. *Let $q > 1$ and $m > 0$ be integers with $\gcd(q,m) = 1$. Let $T \in \mathbb{Z}^+$ be a multiple of $\nu_m(q)$, and let $l \in \mathbb{N}$, $n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$. Then*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \left[{kT + l \atop r}\right]_m \equiv \begin{cases} 2^l (1 - 2^T)^n / m \pmod{q^n} & \text{if } 2 \nmid m, \\ \delta_{l,0} (-1)^r / m \pmod{q^n} & \text{if } 2 \mid m, \end{cases} \tag{1.5}$$

where the Kronecker symbol $\delta_{l,0}$ takes 1 or 0 according as $l = 0$ or not.

Actually Theorem 1.1 is implied by the following more general result whose proof will be given in Section 2.

Theorem 1.2. *Let $q > 1$ be an integer relatively prime to both $m \in \mathbb{Z}^+$ and $\sum_{j=0}^{m-1} (-a)^j$ where $a \in \mathbb{Z}$. Let $l \in \mathbb{N}$ and $r \in \mathbb{Z}$. If $n, T \in \mathbb{Z}^+$ and $\nu_m(q) \mid T$, then we have*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \left[{kT + l \atop r}\right]_m (a) \equiv \frac{(a+1)^l}{m} \left(1 - (a+1)^T\right)^n \pmod{q^n}. \tag{1.6}$$

Now we explain why Theorem 1.1 follows from Theorem 1.2. In the case $2 \nmid m$, since $\sum_{j=0}^{m-1} (-1)^j = 1$ we have (1.5) by applying Theorem 1.2 with $a = 1$. In the case $2 \mid m$, (1.5) also holds because

$$(-1)^r \left[{kT + l \atop r}\right]_m = (-1)^r \left[{kT + l \atop r}\right]_m (1) = \left[{kT + l \atop r}\right]_m (-1)$$

and therefore

$$
\begin{aligned}
&(-1)^r\sum_{k=0}^n(-1)^k\binom{n}{k}\begin{bmatrix}kT+l\\ r\end{bmatrix}_m\\
&=\sum_{k=0}^n(-1)^k\binom{n}{k}\begin{bmatrix}kT+l\\ r\end{bmatrix}_m(-1)\equiv\frac{\delta_{l,0}}{m}\ (\mathrm{mod}\ q^n)
\end{aligned}
$$

with the help of Theorem 1.2 in the case $a=-1$.

Corollary 1.3. *Let $q>1$ and $m>0$ be integers with $\gcd(q,m)=1$. And let $l\in\mathbb{N}$, $n\in\mathbb{Z}^+$ and $r\in\mathbb{Z}$.*

(i) *Let a be any integer with $\gcd(q,\sum_{j=0}^{m-1}(-a)^j)=1$. Then*

$$
\begin{bmatrix}l+\nu_m(q)\\ r\end{bmatrix}_m(a)-\begin{bmatrix}l\\ r\end{bmatrix}_m(a)\equiv\begin{cases}0\ (\mathrm{mod}\ q_0),\\ -(a+1)^l/m\ (\mathrm{mod}\ q/q_0),\end{cases} \tag{1.7}
$$

where q_0 is the largest divisor of q relatively prime to $a+1$. Moreover, for each $k=1,2,3,\ldots$ we have

$$
\begin{aligned}
&\begin{bmatrix}k\nu_m(q)+l\\ r\end{bmatrix}_m(a)-\sum_{j=0}^{n-1}(-1)^{n-1-j}\binom{k-1-j}{n-1-j}\binom{k}{j}\begin{bmatrix}j\nu_m(q)+l\\ r\end{bmatrix}_m(a)\\
&\quad\equiv\frac{(a+1)^l}{m}\sum_{n\leqslant j\leqslant k}\binom{k}{j}\left((a+1)^{\nu_m(q)}-1\right)^j\ (\mathrm{mod}\ q^n).
\end{aligned} \tag{1.8}
$$

(ii) *Suppose that m is even. For any $k\in\mathbb{Z}^+$ we have*

$$
\begin{aligned}
&\begin{bmatrix}k\nu_m(q)+l\\ r\end{bmatrix}_m-\sum_{j=0}^{n-1}(-1)^{n-1-j}\binom{k-1-j}{n-1-j}\binom{k}{j}\begin{bmatrix}j\nu_m(q)+l\\ r\end{bmatrix}_m\\
&\quad\equiv\delta_{l,0}\frac{(-1)^{n+r}}{m}\binom{k-1}{n-1}\ (\mathrm{mod}\ q^n).
\end{aligned} \tag{1.9}
$$

In particular,

$$
\begin{bmatrix}l+\nu_m(q)\\ r\end{bmatrix}_m-\begin{bmatrix}l\\ r\end{bmatrix}_m\equiv\delta_{l,0}\frac{(-1)^{r-1}}{m}\ (\mathrm{mod}\ q). \tag{1.10}
$$

Proof. (i) Suppose that $p^\alpha\| q$ (i.e., $p^\alpha\mid q$ but $p^{\alpha+1}\nmid q$) where p is a prime and $\alpha\in\mathbb{Z}^+$. If $p\mid a+1$, then $p^\alpha|(a+1)^{\nu_m(q)}$ since $\nu_m(q)\geqslant p^{\alpha-1}\geqslant\alpha$; if $p\nmid a+1$, then $(a+1)^{\nu_m(q)}\equiv 1\ (\mathrm{mod}\ p^\alpha)$ as $\varphi(p^\alpha)\mid\nu_m(q)$. Therefore (1.7) follows from (1.6) in the case $n=1$ and $T=\nu_m(q)$. Note that $(a+1)^l\equiv 0\ (\mathrm{mod}\ q/q_0)$ if l is sufficiently large.

Let $k \in \mathbb{Z}^+$. By Lemma 2.1 of [Su],

$$a_k - \sum_{j=0}^{n-1}(-1)^{n-1-j}\binom{k-1-j}{n-1-j}\binom{k}{j}a_j = \sum_{n\leqslant j\leqslant k}\binom{k}{j}(-1)^j\sum_{i=0}^{j}\binom{j}{i}(-1)^i a_i$$

for any sequence $a_0, a_1, \ldots$ of complex numbers. Applying this we immediately obtain (1.8) by noting that

$$\sum_{i=0}^{j}\binom{j}{i}(-1)^i\begin{bmatrix} i\nu_m(q)+l \\ r\end{bmatrix}_m(a) \equiv \frac{(a+1)^l}{m}\left(1-(a+1)^{\nu_m(q)}\right)^j \pmod{q^j}$$

in view of (1.6).

(ii) Applying (1.8) with $a=-1$, we find that

$$\begin{bmatrix} k\nu_m(q)+l \\ r\end{bmatrix}_m(-1) - \sum_{j=0}^{n-1}(-1)^{n-1-j}\binom{k-1-j}{n-1-j}\binom{k}{j}\begin{bmatrix} j\nu_m(q)+l \\ r\end{bmatrix}_m(-1)$$

is congruent to $\delta_{l,0}m^{-1}\sum_{n\leqslant j\leqslant k}\binom{k}{j}(-1)^j$ modulo q^n. Observe that

$$\begin{aligned}\sum_{n\leqslant j\leqslant k}\binom{k}{j}(-1)^j =& \sum_{n\leqslant j\leqslant k}\left(\binom{k-1}{j}(-1)^j - \binom{k-1}{j-1}(-1)^{j-1}\right)\\ =&\binom{k-1}{k}(-1)^k - \binom{k-1}{n-1}(-1)^{n-1} = (-1)^n\binom{k-1}{n-1}.\end{aligned}$$

As $2 \mid m$, we also have

$$\begin{bmatrix} j\nu_m(q)+l \\ r\end{bmatrix}_m(-1) = (-1)^r\begin{bmatrix} j\nu_m(q)+l \\ r\end{bmatrix}_m \quad \text{for } j=0,1,2,\ldots.$$

So (1.9) follows. In the case $k=n=1$, (1.9) yields (1.10). We are done. $\square$

Remark 1.1. Let $q>1$ and $m>0$ be relatively prime integers. Let a be an integer such that $\gcd(1-(-a)^m, q)=1$, or $a \equiv -1 \pmod q$, or $a \equiv 1 \pmod q$ and $2 \mid m$. By Corollary 1.3(i), we have the following extension of Glaisher's periodic result:

$$\begin{bmatrix} n+\nu_m(q) \\ r\end{bmatrix}_m(a) \equiv \begin{bmatrix} n \\ r\end{bmatrix}_m(a) \pmod q \quad \text{for any } n\in\mathbb{Z}^+ \text{ and } r\in\mathbb{Z}. \quad (1.11)$$

(Note that $\begin{bmatrix} n \\ r\end{bmatrix}_m(-a) = (-1)^r\begin{bmatrix} n \\ r\end{bmatrix}_m(a)$ if $2 \mid m$.)

Corollary 1.4. *Let $q>1$ be an integer relatively prime to $m\in\mathbb{Z}^+$. And let $k\in\mathbb{Z}^+$, $l\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then*

$$\begin{aligned}&\begin{bmatrix}k\nu_m(q)+l\\ r\end{bmatrix}_m-k\begin{bmatrix}\nu_m(q)+l\\ r\end{bmatrix}_m+(k-1)\begin{bmatrix}l\\ r\end{bmatrix}_m\\ \equiv&\begin{cases}\delta_{l,0}(-1)^r(k-1)/m \pmod{q^2} & \text{if } 2\mid m,\\ 2^l(2^{k\nu_m(q)}-1-k(2^{\nu_m(q)}-1))/m \pmod{q^2} & \text{if } 2\nmid m.\end{cases}\end{aligned}\tag{1.12}$$

Proof. In the case $2\mid m$, we get the desired congruence by applying (1.9) with $n=2$. When $2\nmid m$, putting $a=1$ in (1.8) we obtain

$$\begin{aligned}&\begin{bmatrix}k\nu_m(q)+l\\ r\end{bmatrix}_m-k\begin{bmatrix}\nu_m(q)+l\\ r\end{bmatrix}_m+(k-1)\begin{bmatrix}l\\ r\end{bmatrix}_m\\ \equiv&\frac{2^l}{m}\sum_{2\leqslant j\leqslant k}\binom{k}{j}(2^{\nu_m(q)}-1)^j=\frac{2^l}{m}(2^{k\nu_m(q)}-1-k(2^{\nu_m(q)}-1)) \pmod{q^2}.\end{aligned}$$

This completes the proof. □

Remark 1.2. Let p be an odd prime. Let $k\in\mathbb{Z}^+$ and $r\in\{0,1,\ldots,p-2\}$. As $\nu_{p-1}(p)=p-1$, by Corollary 1.4 we have

$$\begin{bmatrix}k(p-1)\\ r\end{bmatrix}_{p-1}\equiv k\begin{bmatrix}p-1\\ r\end{bmatrix}_{p-1}-(k-1)\begin{bmatrix}0\\ r\end{bmatrix}_{p-1}+(-1)^r\frac{k-1}{p-1} \pmod{p^2}.$$

As $0\leqslant r<p-1$ and $1/(p-1)\equiv -p-1 \pmod{p^2}$, this turns out to be

$$\begin{bmatrix}k(p-1)\\ r\end{bmatrix}_{p-1}\equiv k\binom{p-1}{r}-(-1)^r(k-1)(p+1)+\delta_{r,0} \pmod{p^2}.\tag{1.13}$$

In the case $r=0$, this solves a problem proposed by V. Dimitrov [Di].

Let p be any odd prime and let $\alpha,n\in\mathbb{Z}^+$. As $\nu_{p-1}(p^\alpha)=p^\alpha-p^{\alpha-1}$, by Remark 1.1 we have

$$\begin{bmatrix}p^\alpha n\\ r\end{bmatrix}_{p-1}\equiv\begin{bmatrix}p^{\alpha-1}n\\ r\end{bmatrix}_{p-1} \pmod{p^\alpha}\ \ \text{for any } r\in\mathbb{Z}.\tag{1.14}$$

In 1953, by using some deep properties of Bernoulli numbers, L. Carlitz [C] extended Hermite's congruence in the following way:

$$p+(p-1)\sum_{\substack{0<k<p^{\alpha-1}n\\ p-1\mid k}}\binom{p^{\alpha-1}n}{k}\equiv 0 \pmod{p^\alpha}.$$

When $p-1 \mid n$, this follows from (1.10), for, $\nu_{p-1}(p^\alpha)$ divides $p^{\alpha-1}n$ and hence

$$\begin{bmatrix} p^{\alpha-1}n \\ 0 \end{bmatrix}_{p-1} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix}_{p-1} - \frac{1}{p-1} = 1 - \frac{1}{p-1} \pmod{p^\alpha}.$$

Let $q > 1$ and $m > 0$ be integers with $\gcd(q,m) = 1$. Let a be an integer with $\gcd(1-(-a)^m, q) = 1$, or $a \equiv -1 \pmod q$, or $a \equiv 1 \pmod q$ and $2 \mid m$. What is the smallest positive integer $\mu_m(a,q)$ such that

$$\begin{bmatrix} n+\mu_m(a,q) \\ r \end{bmatrix}_m (a) \equiv \begin{bmatrix} n \\ r \end{bmatrix}_m (a) \pmod q \tag{1.15}$$

holds for all $n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$? Clearly $\mu_m(0,q) = 1$, and $\mu_m(a,q) | \nu_m(q)$ by (1.11). (If $\mu_m(a,q) \nmid \nu_m(q)$, then the least positive residue of $\nu_m(q)$ mod $\mu_m(a,q)$ would be a period smaller than $\mu_m(a,q)$.)

Conjecture 1.5. *Let $q > 1$ and $m > 0$ be integers with $\gcd(q,m) = 1$ and $q \not\equiv 0 \pmod 3$. Then $\nu_m(q)$ is the maximal value of $\mu_m(a,q)$, where a is an integer with $\gcd(1-(-a)^m, q) = 1$, or $a \equiv -1 \pmod q$, or $a \equiv 1 \pmod q$ and $2 \mid m$.*

Now we give an example to illustrate our conjecture.

Example 1.1. (i) Since the order of 3 modulo 7 is 6, we have $\nu_7(9) = 3(3^6-1) = 2184$. For any given $a \in \mathbb{Z}$, clearly

$$1-(-a)^7 = 1 + a^3a^3a \equiv 1 + a^3 \equiv 1 + a \pmod 3$$

since $a^3 \equiv a \pmod 3$, thus $\gcd(1-(-a)^7, 9) = 1$ if and only if $a \not\equiv 2 \pmod 3$. Through computation we obtain that

$$\mu_7(-1,9) = 1092,\ \mu_7(1,9) = \mu_7(-2,9) = \mu_7(4,9) = 546,\ \mu_7(\pm 3,9) = 3.$$

(ii) The order of 5 modulo 7 is 6, thus $\nu_7(5) = 5^6 - 1 = 15624$. For any given $a \in \mathbb{Z}$, clearly $1-(-a)^7 = 1 + a^5a^2 \equiv 1 + a^3 \pmod 5$, thus $5 \nmid 1-(-a)^7$ if and only if $a \not\equiv -1 \pmod 5$. By computation we find that

$$\mu_7(1,5) = 868,\ \mu_7(-1,5) = 1736,\ \mu_7(2,5) = 2232,\ \mu_7(-2,5) = 15624.$$

(iii) Clearly $\nu_6(11) = 11^2 - 1 = 120$. By computation, $\mu_6(\pm 1, 11) = 60$ and $\mu_6(a,11) = 120$ for any integer $a \not\equiv 0, \pm 1 \pmod{11}$. Note that $4(a^4 + a^2 + 1) = (2a^2+1)^2 + 3 \not\equiv 0 \pmod{11}$ since -3 is a quadratic non-residue modulo 11. Thus, if $a \not\equiv \pm 1 \pmod{11}$ then $1-(-a)^6 = (1-a^2)(a^4+a^2+1)$ is relatively prime to 11.

2. Proof of Theorem 1.2

In this section we work with congruences in the ring of algebraic integers. The reader may consult [IR, pp. 66–69] for the basic knowledge of algebraic integers.

Lemma 2.1. *Let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, and let $q > 1$ be an integer relatively prime to $m\sum_{j=0}^{m-1}(-a)^j$. If $\zeta \neq 1$ is an m-th root of unity, then we have the congruence*

$$(1+a\zeta)^{\nu_m(q)} \equiv 1 \pmod{q} \tag{2.1}$$

in the ring of algebraic integers.

Proof. Let p be any prime divisor of q, and let β be the order of p modulo m. Below we use induction to show that

$$(1+a\zeta)^{p^{\alpha-1}(p^\beta-1)} \equiv 1 \pmod{p^\alpha} \tag{2.2}$$

for every $\alpha = 1, 2, 3, \ldots$.

Since $p \mid \binom{p}{k}$ for $k = 1, \ldots, p-1$ and $a^p \equiv a \pmod{p}$ by Fermat's little theorem, we have

$$(1+a\zeta)^p = 1 + a^p\zeta^p + \sum_{k=1}^{p-1}\binom{p}{k}(a\zeta)^k \equiv 1 + a\zeta^p \pmod{p},$$

hence

$$(1+a\zeta)^{p^2} \equiv (1+a\zeta^p)^p \equiv 1 + a\zeta^{p^2} \pmod{p}$$

and so on. Thus

$$(1+a\zeta)^{p^\beta} \equiv 1 + a\zeta^{p^\beta} = 1 + a\zeta \pmod{p}.$$

(Recall that $p^\beta \equiv 1 \pmod{m}$ and $\zeta^m = 1$.) Clearly

$$\prod_{0<j<m}\frac{1+ae^{2\pi ij/m}}{-e^{2\pi ij/m}} = \prod_{0<j<m}(x - e^{-2\pi ij/m})\Big|_{x=-a}$$
$$= \lim_{x\to -a}\frac{x^m-1}{x-1} = \sum_{j=0}^{m-1}(-a)^j$$

and so $z = 1 + a\zeta$ divides $c = \sum_{j=0}^{m-1}(-a)^j$ in the ring of algebraic integers. Therefore

$$cz^{p^\beta-1} \equiv \frac{c}{z}z^{p^\beta} \equiv \frac{c}{z}z \equiv c \pmod{p}$$

and hence $z^{p^\beta-1} \equiv 1 \pmod{p}$ since $p \nmid c$. This proves (2.2) in the case $\alpha = 1$.

Now let $\alpha \in \mathbb{Z}^+$ and suppose that (2.2) holds. Then $z^{p^{\alpha-1}(p^\beta-1)} = 1 + p^\alpha\omega$ for some algebraic integer ω. It follows that

$$z^{p^\alpha(p^\beta-1)} = (1+p^\alpha\omega)^p \equiv 1 + \binom{p}{1}p^\alpha\omega \equiv 1 \pmod{p^{\alpha+1}}.$$

This concludes the induction step.

For any $q_1, q_2 \in \mathbb{Z}$ with $\gcd(q_1, q_2) = 1$, there are $x_1, x_2 \in \mathbb{Z}$ such that $q_1x_1 + q_2x_2 = 1$, If an algebraic integer ω is divisible by both q_1 and q_2, then $\omega = q_1(\omega x_1) + q_2(\omega x_2)$ is divisible by q_1q_2 in the ring of algebraic integers. Therefore (2.1) is valid in view of what we have proved. $\square$

Remark 2.1. Write an integer $q > 1$ in the form $p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, where $p_1, \ldots, p_t$ are distinct primes and $\alpha_1, \ldots, \alpha_t \in \mathbb{Z}^+$. Let m be a positive integer dividing $p_s - 1$ for all $s = 1, \ldots, t$. And let g be an integer with $g \equiv g_s^{\varphi(p_s^{\alpha_s})/m} \pmod{p_s^{\alpha_s}}$ for $s = 1, \ldots, t$, where g_s is a primitive root modulo p_s. Clearly $g^m \equiv 1 \pmod q$. Suppose that $j \in \mathbb{Z}^+$ and $j < m$. Then $p_s - 1 \nmid j\varphi(p_s^{\alpha_s})/m$ and hence $g^j \not\equiv 1 \pmod{p_s}$. Therefore $\gcd(g^j - 1, q) = 1$. If $p_s \mid 1 + ag^j$, then $-a \equiv g^{m-j} \not\equiv 1 \pmod{p_s}$ but $(a+1)\sum_{i=0}^{m-1}(-a)^i = 1 - (-a)^m \equiv 1 - g^{(m-j)m} \equiv 0 \pmod{p_s}$. Thus, if $\gcd(\sum_{i=0}^{m-1}(-a)^i, q) = 1$, then $\gcd(1 + ag^j, q) = 1$, and hence

$$(1 + ag^j)^{\nu_m(q)} \equiv 1 \pmod q \tag{2.3}$$

which is an analogue of (2.1).

Proof of Theorem 1.2. Set $\zeta = e^{2\pi i/m}$. For any $h \in \mathbb{Z}$, we clearly have

$$\sum_{j=0}^{m-1} \zeta^{jh} = \begin{cases} m & \text{if } m \mid h, \\ 0 & \text{otherwise.} \end{cases}$$

If $n \in \mathbb{N}$ then

$$\begin{aligned} m\begin{bmatrix} n \\ r \end{bmatrix}_m(a) &= \sum_{k=0}^{n}\binom{n}{k}a^k\sum_{j=0}^{m-1}\zeta^{j(k-r)} \\ &= \sum_{j=0}^{m-1}\zeta^{-jr}\sum_{k=0}^{n}\binom{n}{k}a^k\zeta^{jk} = \sum_{j=0}^{m-1}\zeta^{-jr}(1+a\zeta^j)^n. \end{aligned}$$

Now let $T \in \mathbb{Z}^+$ be a multiple of $\nu_m(q)$, and fix a positive integer n. By the above,

$$\begin{aligned}
& m\sum_{k=0}^{n}(-1)^k\binom{n}{k}\begin{bmatrix}kT+l\\ r\end{bmatrix}_m(a) \\
=& \sum_{j=0}^{m-1}\zeta^{-jr}\sum_{k=0}^{n}\binom{n}{k}(-1)^k(1+a\zeta^j)^{kT+l} \\
=& \sum_{j=0}^{m-1}\zeta^{-jr}(1+a\zeta^j)^l\left(1-(1+a\zeta^j)^T\right)^n \\
\equiv& (1+a)^l\left(1-(1+a)^T\right)^n \pmod{q^n}
\end{aligned}$$

where we have applied Lemma 2.1. This concludes our proof. □

Remark 2.2. Let $a, r \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, and let $q > 1$ be an integer relatively prime to $\sum_{j=0}^{m-1}(-a)^j$. Suppose that $m \mid p-1$ for any prime divisor p of q. Obviously $\gcd(m, q) = 1$. Choose $g \in \mathbb{Z}$ as in Remark 2.1. Then $g^m \equiv 1 \pmod q$, and for each $0 < j < m$ we have $\gcd(g^j - 1, q) = 1$ as well as (2.3). By modifying the proof of Theorem 1.2 slightly, we find that

$$m\begin{bmatrix}n\\ r\end{bmatrix}_m(a) \equiv \sum_{j=0}^{m-1} g^{-jr}(1+ag^j)^n = (a+1)^n + \sum_{0<j<m} g^{-jr}a_j^n \pmod q$$

for every $n \in \mathbb{N}$, where $a_j = 1 + ag^j$ $(0 < j < m)$ are relatively prime to q. If $q \mid a+1$ or $\gcd(a+1, q) = 1$, then the function $f : \mathbb{Z}^+ \to \mathbb{Z}$ given by $f(n) = \left[{n \atop r}\right]_m(a)$ is q-normal in the sense that

$$f(n) \equiv \sum_{\substack{1\leqslant j<q\\ \gcd(j,q)=1}} c_j j^n \pmod q \quad \text{for all } n \in \mathbb{Z}^+, \tag{2.4}$$

where c_j $(1 \leqslant j < q$ and $\gcd(j, q) = 1)$ are suitable integers. The concept of q-normal function was first introduced by Sun [S03] where the reader can find some q-normal functions involving Bernoulli polynomials.

Acknowledgments. The joint work was done during the first author's stay at Univ. Lyon-I as a visiting professor, thus he is indebted to Prof. J. Zeng for the invitation and hospitality. The authors also thank the referee for his/her helpful comments.

References

[AKS] M. Agrawal, N. Kayal and N. Saxena, *Primes is in P*, Ann. of Math. (2) **160** (2004), 781–793.

[C] L. Carlitz, *A special congruence*, Proc. Amer. Math. Soc. **4** (1953), 933–936.

[D] L. E. Dickson, *History of the Theory of Numbers,* Vol. I, AMS Chelsea Publ., 1999.

[Di] V. Dimitrov, *Problem 11118*, Amer. Math. Monthly **111** (2004), no. 10, 915.

[G97] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers,* in: Organic mathematics (Burnady, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.

[G05] A. Granville, *It is easy to determine whether a given integer is prime*, Bull. Amer. Math. Soc. **42** (2005), 3–38.

[GS] A. Granville and Z. W. Sun, *Values of Bernoulli polynomials*, Pacific J. Math. **172** (1996), 117–138.

[H] C. Helou, *Norm residue symbol and cyclotomic units*, Acta Arith. **73** (1995), 147–188.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in math.; 84), 2nd ed., Springer, New York, 1990.

[Su] Z. H. Sun, *Congruences for Bernoulli numbers and Bernoulli polynomials*, Discrete Math. **163** (1997), 153–163.

[SS] Z. H. Sun and Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371–388.

[S95] Z. W. Sun, *A congruence for primes*, Proc. Amer. Math. Soc. **123** (1995), 1341–1346.

[S02] Z. W. Sun, *On the sum* $\sum_{k\equiv r\,(\mathrm{mod}\ m)}\binom{n}{k}$ *and related congruences*, Israel J. Math. **128** (2002), 135–156.

[S03] Z. W. Sun, *General congruences for Bernoulli polynomials*, Discrete Math. **262** (2003), 253–276.