ACTA ARITHMETICA
XCVII.1 (2001)

Products of binomial coefficients modulo p^2

by

Zhi-Wei Sun (Nanjing)

1. Introduction. As usual $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the ring of integers, the rational field, the real field and the complex field respectively. We also let $\mathbb{Z}^+ = \{1, 2, \ldots\}$ and $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, by (a, n) we mean the greatest common divisor of a and n. If n is odd then the Jacobi symbol $(\frac{a}{n})$ is defined in terms of Legendre symbols (see, e.g., [IR]). For $x \in \mathbb{R}$, $[x]$ and $\{x\}$ stand for the integral and the fractional parts of x respectively. For a prime p and an integer a prime to p, the Fermat quotient $(a^{p-1} - 1)/p$ is denoted by $q_p(a)$. For an odd prime p and $a \in \mathbb{Z}$, we define the *Euler quotient*

$$\mathrm{eq}_p(a) = \frac{a^{(p-1)/2} - (\frac{a}{p})}{p}. \tag{1.1}$$

The Gauss lemma used to prove the law of quadratic reciprocity is as follows:

Gauss's Lemma. *Let $n > 0$ be an odd integer and a an integer prime to n. Then*

$$\left(\frac{a}{n}\right) = (-1)^{|S_n(a)|} \quad \textit{where } S_n(a) = \left\{k \in \mathbb{Z}^+ : \frac{k}{n} < \frac{1}{2} < \left\{\frac{ka}{n}\right\}\right\}. \tag{1.2}$$

Almost every textbook on number theory only contains Gauss's Lemma with $n = p$ being an odd prime. The general version of Gauss's Lemma was first published by M. Jenkins [J] in 1867 with an elementary proof; in the textbook [R] H. Rademacher supplied a proof using subtle properties of quadratic Gauss sums.

2000 *Mathematics Subject Classification*: Primary 11B65; Secondary 11A07, 11B68.

The research is supported by the Teaching and Research Award Fund for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of P.R. China.

For $x \in \mathbb{R}$ let

$$\binom{x}{0} = 1 \quad \text{and} \quad \binom{x}{n} = \frac{1}{n!}\prod_{j=0}^{n-1}(x-j) \quad \text{for } n = 1, 2, \ldots$$

Recently A. Granville [G] obtained a congruence for $\prod_{0<k<n}\binom{p-1}{[pk/n]} \bmod p^2$ where p is an odd prime not dividing $n \in \mathbb{Z}^+$. With the help of Gauss's Lemma, we are able to get the following more general result.

THEOREM 1.1. *Let $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Let p be an odd prime not dividing n.*

(i) *If $\delta \in \{0,1\}$ then*

$$(1.3) \quad (-1)^{\frac{p-1}{2}[\frac{n-\delta}{2}]} \prod_{0<k\le[(n-\delta)/2]} \binom{pm-1}{[pk/n]}$$

$$\equiv \begin{cases} \left(\frac{n}{p}\right) + pmn\,\mathrm{eq}_p(n) \pmod{p^2} & \text{if } 2\nmid n, \\ \left(\frac{2n}{p}\right) + pm\big((-1)^\delta\left(\frac{n}{p}\right)2\,\mathrm{eq}_p(2) + \left(\frac{2}{p}\right)n\,\mathrm{eq}_p(n)\big) \pmod{p^2} & \text{if } 2\mid n. \end{cases}$$

(ii) *We have*

$$(1.4) \quad \sum_{k=0}^{n-1}(-1)^{k+(n-1)[pk/n]}\binom{pm-1}{[pk/n]}$$

$$\equiv \begin{cases} mn(1-2^{p-1}) \pmod{p^2} & \text{if } 2\mid n, \\ 1 \pmod{p^2} & \text{if } 2\nmid n. \end{cases}$$

REMARK 1.1. In (1.3) we use Euler quotients instead of Fermat quotients, this makes the congruence somewhat symmetric in the case $2\mid n$.

Now we deduce Granville's result from our Theorem 1.1.

COROLLARY 1.1 (Granville [G]). *Let n be a positive integer and p an odd prime not dividing n. Then*

$$(1.5) \quad \prod_{0<k<n}\binom{p-1}{[pk/n]} \equiv (-1)^{\frac{p-1}{2}(n-1)}(n^p - n + 1) \pmod{p^2}.$$

Proof. Observe that

$$(-1)^{\frac{p-1}{2}(n-1)}\prod_{0<k<n}\binom{p-1}{[pk/n]}$$

$$= (-1)^{\frac{p-1}{2}([\frac{n-1}{2}]+[\frac{n}{2}])}\prod_{0<k\le[(n-1)/2]}\binom{p-1}{[pk/n]} \cdot \prod_{0<k\le[n/2]}\binom{p-1}{[p(n-k)/n]}$$

$$= (-1)^{\frac{p-1}{2}[\frac{n-1}{2}]}\prod_{0<k\le[(n-1)/2]}\binom{p-1}{[pk/n]} \cdot (-1)^{\frac{p-1}{2}[\frac{n}{2}]}\prod_{0<k\le[n/2]}\binom{p-1}{[pk/n]}.$$

Applying Theorem 1.1(i) with $m=1$ and $\delta=0,1$, we then obtain

$$(-1)^{\frac{p-1}{2}(n-1)}\prod_{0<k<n}\binom{p-1}{[pk/n]}\equiv 1+2pn\left(\frac{n}{p}\right)\mathrm{eq}_p(n)\pmod{p^2}.$$

For any integer a prime to p, clearly

$$a^{p-1}-1=\left(a^{(p-1)/2}+\left(\frac{a}{p}\right)\right)\left(a^{(p-1)/2}-\left(\frac{a}{p}\right)\right)\equiv 2\left(\frac{a}{p}\right)p\,\mathrm{eq}_p(a)\pmod{p^2}.$$

So (1.5) follows. ■

For $a,n\in\mathbb{Z}$ with $0\le a<n$, we let

$$a(n)=a \bmod n=a+n\mathbb{Z}=\{a+nx:x\in\mathbb{Z}\}.$$

For a finite system $A=\{a_s(n_s)\}_{s=1}^k$ of such residue classes, we define the *covering function* $w_A:\mathbb{Z}\to\{0,1,\ldots\}$ by

$$w_A(x)=|\{1\le s\le k:x\in a_s(n_s)\}|. \tag{1.6}$$

When $w_A(x)=m$ for all $x\in\mathbb{Z}$, A is said to be an *exact m-cover* (of $\mathbb{Z}$). We also use the term *disjoint cover* instead of exact 1-cover. (See [S3] and [S4] for problems and results on covers of $\mathbb{Z}$.) For two systems A and B of residue classes, if $w_A=w_B$, then we say that A is *covering equivalent* to B, and denote this by $A\sim B$. For $d,n\in\mathbb{Z}^+$ and $a\in\{0,1,\ldots,d-1\}$, clearly

$$\{a+jd(nd)\}_{j=0}^{n-1}\sim\{a(d)\}, \tag{1.7}$$

in particular $\{r(n)\}_{r=0}^{n-1}\sim\{0(1)\}$.

In this paper we will also prove the following extension of Corollary 1.1.

Theorem 1.2. *Let p be an odd prime. Let $A=\{a_s(n_s)\}_{s=1}^k$ $(0\le a_s<n_s)$ and $B=\{b_t(m_t)\}_{t=1}^l$ $(0\le b_t<m_t)$ be covering equivalent systems with the moduli n_s and m_t not divisible by p but dividing an integer N. Then for any $x\in[0,p)$ we have*

$$\prod_{s=1}^k\binom{pN/n_s-1}{[(x+pa_s)/n_s]}\Big/\prod_{t=1}^l\binom{pN/m_t-1}{[(x+pb_t)/m_t]} \equiv(-1)^{(k-l)(p-1)/2}\left(1+pN\left(\sum_{s=1}^k\frac{q_p(n_s)}{n_s}-\sum_{t=1}^l\frac{q_p(m_t)}{m_t}\right)\right)\pmod{p^2}. \tag{1.8}$$

Remark 1.2. Actually we may not require the integer N in Theorem 1.2 to be a common multiple of those moduli n_s and m_t. For example $N=1$ is allowed if we do not mind using $x\notin\mathbb{Z}$ in the notation $\binom{x}{n}$.

Corollary 1.2. *Let $A=\{a_s(n_s)\}_{s=1}^k$ $(0\le a_s<n_s)$ be an exact m-cover of $\mathbb{Z}$. Let N be the least common multiple of $n_1,\ldots,n_k$ and p an*

odd prime not dividing N. *Then*

$$\prod_{s=1}^{k}\binom{pN/n_s-1}{[pa_s/n_s]}\equiv(-1)^{(k-m)(p-1)/2}\left(1+pN\sum_{s=1}^{k}\frac{q_p(n_s)}{n_s}\right)\pmod{p^2}. \tag{1.9}$$

Proof. Let B be the system consisting of m copies of $0(1)$. Then $A\sim B$. Since $\left[\frac{p0}{1}\right]=\frac{q_p(1)}{1}=0$, Corollary 1.2 follows immediately from Theorem 1.2. ■

REMARK 1.3. Applying Corollary 1.2 to the trivial disjoint cover $A=\{r(n)\}_{r=0}^{n-1}$ we then get Corollary 1.1 again.

In the next section we will give some examples of uniform maps the concept of which arose from our previous study of covering equivalence (cf. [S1] and [S2]). On the basis of Section 2, we prove Theorems 1.1 and 1.2 in Section 3.

2. Some uniform maps

DEFINITION 2.1. Let m be an integer and M an additive abelian group. Let f be a map from a subset of $\mathbb{C}\times\mathbb{C}$ into M. If for any ordered pair $\langle x,y\rangle$ in the domain $\mathrm{Dom}(f)$ of f and each positive integer n prime to m, we have

$$\left\{\left\langle\frac{x+mr}{ny},ny\right\rangle : r=0,1,\ldots,n-1\right\}\subseteq\mathrm{Dom}(f) \tag{2.1}$$

and

$$\sum_{r=0}^{n-1}f\left(\frac{x+mr}{n},ny\right)=f(x,y), \tag{2.2}$$

then we call f an *m-uniform map* (into M).

The functional equation (2.2) with $m=1$ was first introduced by the author in [S1] where he showed the following theorem in the case $m=1$ by a complicated induction method.

THEOREM 2.1. *Let m be an integer and M a left R-module where R is a ring with identity. Let f be a map into M with* $\mathrm{Dom}(f)\subseteq\mathbb{C}\times\mathbb{C}$ *such that* (2.1) *holds for any* $\langle x,y\rangle\in\mathrm{Dom}(f)$ *and* $n\in\mathbb{Z}^+$ *with* $(m,n)=1$. *Then the following two statements are equivalent*:

(a) *f is an m-uniform map into M.*

(b) *Whenever*

$$\sum_{\substack{1\le s\le k\\ x\in a_s(n_s)}}\lambda_s=\sum_{\substack{1\le t\le l\\ x\in b_t(m_t)}}\mu_t\qquad\textit{for all } x\in\mathbb{Z} \tag{2.3}$$

(*with* $\lambda_s,\mu_t \in R$, $a_s,n_s,b_t,m_t \in \mathbb{Z}$, $0 \le a_s < n_s$, $0 \le b_t < m_t$ *and* $(n_s m_t, m) = 1$), *we have*

$$\sum_{s=1}^{k} \lambda_s f\left(\frac{x+ma_s}{n_s}, n_s y\right) = \sum_{t=1}^{l} \mu_t f\left(\frac{x+mb_t}{m_t}, m_t y\right) \tag{2.4}$$

for $\langle x,y\rangle \in \mathrm{Dom}(f)$.

Proof. Since $\{r(n)\}_{r=0}^{n-1} \sim \{0(1)\}$ for all $n \in \mathbb{Z}^+$, (b) implies (a).

Now we show (b) under the condition (a). Suppose that (2.3) holds. Let N be the least common multiple of those moduli n_s and m_t. If $\langle x,y\rangle \in \mathrm{Dom}(f)$, then

$$\begin{aligned}
&\sum_{s=1}^{k} \lambda_s f\left(\frac{x+ma_s}{n_s}, n_s y\right) \\
&= \sum_{s=1}^{k} \lambda_s \sum_{j=0}^{N/n_s-1} f\left(\frac{(x+ma_s)/n_s + jm}{N/n_s}, \frac{N}{n_s}(n_s y)\right) \\
&= \sum_{s=1}^{k} \lambda_s \sum_{\substack{r=0\\ r\in a_s(n_s)}}^{N-1} f\left(\frac{x+mr}{N}, Ny\right) = \sum_{r=0}^{N-1} \Big(\sum_{\substack{1\le s\le k\\ r\in a_s(n_s)}} \lambda_s\Big) f\left(\frac{x+mr}{N}, Ny\right) \\
&= \sum_{r=0}^{N-1} \Big(\sum_{\substack{1\le t\le l\\ r\in b_t(m_t)}} \mu_t\Big) f\left(\frac{x+mr}{N}, Ny\right) = \sum_{t=1}^{l} \mu_t f\left(\frac{x+mb_t}{m_t}, m_t y\right). \blacksquare
\end{aligned}$$

PROPOSITION 2.1. (i) *Let* $m \in \mathbb{Z}$. *Then the function* $[\ ]_m : \mathbb{R}\times\mathbb{R} \to \mathbb{Q}$ *given by*

$$[\ ]_m(x,y) = [x] + \frac{1-m}{2} \tag{2.5}$$

is an m*-uniform map into the rational field* $\mathbb{Q}$.

(ii) *For each* $m = 0,1,\ldots$ *the functions* $b_m : \mathbb{C}\times\mathbb{C}^* \to \mathbb{C}$ *and* $e_m : \mathbb{C}\times\mathbb{Z} \to \mathbb{C}$ *given by*

$$b_m(x,y) = y^{m-1} B_m(x) \tag{2.6}$$

and

$$e_m(x,y) = \begin{cases} e^{\pi i x y} y^m E_m(x) & \text{if } y \text{ is odd},\\ -\dfrac{2}{m+1} e^{\pi i x y} y^m B_{m+1}(x) & \text{if } y \text{ is even}, \end{cases} \tag{2.7}$$

are 1*-uniform maps into the complex field* $\mathbb{C}$, *where* $B_m(x)$ *and* $E_m(x)$ *are the* m*th Bernoulli polynomial and the* m*th Euler polynomial respectively.*

Proof. Let n be any positive integer.

(i) If $(m,n)=1$ then

$$\sum_{r=0}^{n-1}\left(\left[\frac{x+mr}{n}\right]+\frac{1-m}{2}\right)$$
$$=\sum_{r=0}^{n-1}\left(\frac{x+mr}{n}+\frac{1-m}{2}-\left\{\frac{x+mr}{n}\right\}\right)$$
$$=x+m\sum_{r=0}^{n-1}\left(\frac{r}{n}-\frac{1}{2}\right)-\sum_{r=0}^{n-1}\left(\left\{\frac{\{x\}+[x]+mr}{n}\right\}-\frac{1}{2}\right)$$
$$=x-\frac{m}{2}-\sum_{s=0}^{n-1}\left(\frac{\{x\}+s}{n}-\frac{1}{2}\right)=x-\frac{m}{2}-\left(\{x\}-\frac{1}{2}\right)=[x]+\frac{1-m}{2}.$$

(ii) Let m be a nonnegative integer. Raabe's identity states that

$$\sum_{r=0}^{n-1}B_m\left(z+\frac{r}{n}\right)=n^{1-m}B_m(nz). \tag{2.8}$$

Another known identity (cf. [B]) asserts that

$$E_m(nz)=\begin{cases} n^m\sum_{r=0}^{n-1}(-1)^rE_m\left(z+\frac{r}{n}\right) & \text{if } 2\nmid n,\\ -\frac{2n^m}{m+1}\sum_{r=0}^{n-1}(-1)^rB_{m+1}\left(z+\frac{r}{n}\right) & \text{if } 2\mid n.\end{cases} \tag{2.9}$$

By these two identities we can easily check that

$$\sum_{r=0}^{n-1}b_m\left(\frac{x+r}{n},ny\right)=b_m(x,y)\quad \text{for } x\in\mathbb{C} \text{ and } y\in\mathbb{C}^*$$

and

$$\sum_{r=0}^{n-1}e_m\left(\frac{x+r}{n},ny\right)=e_m(x,y)\quad \text{for } x\in\mathbb{C} \text{ and } y\in\mathbb{Z}. \ \blacksquare$$

Remark 2.1. In [S1] the author briefly mentioned the basic things for Proposition 2.1. For more examples of 1-uniform maps, the reader is referred to [S5].

Corollary 2.1. *Let p be an odd prime and $n>0$ an even integer prime to p. Then*

$$\sum_{r=0}^{n-1}(-1)^rB_{p-1}\left(\frac{r}{n}\right)\equiv -nq_p(2) \pmod p. \tag{2.10}$$

Proof. By Proposition 2.1,

$$\frac{2n^{p-2}}{1-p}\sum_{r=0}^{n-1}(-1)^r B_{p-1}\left(\frac{r}{n}\right)=\sum_{r=0}^{n-1}e_{p-2}\left(\frac{r}{n},n\right)=e_{p-2}(0,1)$$

does not depend on the value of the positive even integer n. So

$$n^{p-2}\sum_{r=0}^{n-1}(-1)^r B_{p-1}\left(\frac{r}{n}\right)=2^{p-2}\left(2B_{p-1}-\sum_{r=0}^{2-1}B_{p-1}\left(\frac{r}{2}\right)\right)$$
$$=2^{p-1}B_{p-1}-B_{p-1}.$$

Since

$$pB_{p-1}\equiv\sum_{r=1}^{p-1}r^{p-1}\equiv -1 \pmod p$$

(see, e.g., [IR]), (2.10) follows at once. ∎

PROPOSITION 2.2. *Let p be an odd prime. For $x\ge 0$ and $m\in\mathbb{Z}\setminus p\mathbb{Z}$ let*

$$q(x,m)=\frac{q_p(m)}{m}+\sum_{\substack{0<j\le[x]\\ p\nmid j}}\frac{1}{jm}. \tag{2.11}$$

Then the function $\overline{q}(x,m)=q(x,m) \bmod p$ is a p-uniform map into the finite field $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let $m\in\mathbb{Z}\setminus p\mathbb{Z}$ and $n\in\mathbb{Z}^+\setminus p\mathbb{Z}$. Since

$$q_p(mn)=\frac{m^{p-1}-1}{p}+m^{p-1}\frac{n^{p-1}-1}{p}\equiv q_p(m)+q_p(n) \pmod p,$$

for $x\ge 0$ the congruence

$$\sum_{k=0}^{n-1}q\left(\frac{x+pk}{n},nm\right)\equiv q(x,m) \pmod p$$

is equivalent to

$$q_p(n)\equiv\sum_{\substack{0<j\le[x]\\ p\nmid j}}\frac{1}{j}-\frac{1}{n}\sum_{k=0}^{n-1}\sum_{\substack{0<j\le[(x+pk)/n]\\ p\nmid j}}\frac{1}{j} \pmod p. \tag{2.12}$$

Now it suffices to show (2.12) for all $x=0,1,\ldots$

By pp. 125–126 of [GS] we have

$$B_{p-1}\left(\left\{\frac{pk}{n}\right\}\right)-B_{p-1}\equiv-\sum_{0<j\le[pk/n]}\frac{1}{j} \pmod p \tag{2.13}$$

for $k=0,1,\ldots,n-1$.

Observe that

$$\begin{aligned}\sum_{k=0}^{n-1}\left(B_{p-1}\left(\left\{\frac{pk}{n}\right\}\right)-B_{p-1}\right)&\\ &=\sum_{r=0}^{n-1}B_{p-1}\left(\frac{r}{n}\right)-nB_{p-1}=n^{2-p}B_{p-1}-nB_{p-1}\\ &=\frac{n}{n^{p-1}}\cdot\frac{1-n^{p-1}}{p}(pB_{p-1})\equiv nq_p(n)\ (\mathrm{mod}\,p).\end{aligned}$$

Thus (2.12) holds for $x=0$.

Let $r\in\mathbb{Z}^+$. Assume (2.12) for $x=r-1$. Denote by k_0 the unique integer $k\in[0,n)$ such that $r+pk\equiv 0\ (\mathrm{mod}\,n)$. Clearly $p\,|\,r$ if and only if p divides $j_0=(r+pk_0)/n$. For $k\in\{0,1,\dots,n-1\}$, we have

$$\left[\frac{r+pk}{n}\right]=\left[\frac{r-1+pk}{n}\right]+\begin{cases}1 & \text{if } k=k_0,\\ 0 & \text{otherwise.}\end{cases}$$

If $p\nmid r$, then

$$\frac{1}{r}-\frac{1}{n}\cdot\frac{1}{j_0}=\frac{1}{r}-\frac{1}{r+pk_0}\equiv 0\ (\mathrm{mod}\,p).$$

Thus

$$\begin{aligned}\sum_{\substack{0<j\le r\\ p\nmid j}}\frac{1}{j}-\frac{1}{n}\sum_{k=0}^{n-1}\sum_{\substack{0<j\le[(r+pk)/n]\\ p\nmid j}}\frac{1}{j}&\\ \equiv\sum_{\substack{0<j\le r-1\\ p\nmid j}}\frac{1}{j}-\frac{1}{n}\sum_{k=0}^{n-1}\sum_{\substack{0<j\le[(r-1+pk)/n]\\ p\nmid j}}\frac{1}{j}&\equiv q_p(n)\ (\mathrm{mod}\,p).\end{aligned}$$

This concludes the induction step. We are done. ∎

3. Proofs of Theorems 1.1 and 1.2

LEMMA 3.1. (i) *Let $a\in\mathbb{Z}$, $n\in\mathbb{Z}^+$ and $(2a,n)=1$. Then*

$$|S_n(a)|\equiv\sum_{0<k<n/2}\left[\frac{ka}{n}\right]+\frac{n^2-1}{8}(a-1)\ (\mathrm{mod}\,2).\tag{3.1}$$

(ii) *Let $m,n\in\mathbb{Z}^+$ and $(m,n)=1$. Then for $\delta\in\{0,1\}$ we have*

$$\sum_{0<k\le(n-\delta)/2}\left[\frac{km}{n}\right]+\sum_{0<k\le(m-\delta)/2}\left[\frac{kn}{m}\right]=\left[\frac{m-\delta}{2}\right]\left[\frac{n-\delta}{2}\right].\tag{3.2}$$

The above lemma is well known and usually stated in textbooks with a,m,n being odd primes.

LEMMA 3.2. *Let $k, m, n \in \mathbb{Z}$ and $0 \le k < n$. Let p be an odd prime not dividing n. Then*

$$(3.3)\qquad (-1)^{[pk/n]}\binom{pm-1}{[pk/n]} \equiv 1 + pm\left(B_{p-1}\left(\left\{\frac{pk}{n}\right\}\right) - B_{p-1}\right) \pmod{p^2}.$$

Proof. For any $l \in \{0, 1, \dots, p-1\}$,

$$(3.4)\qquad (-1)^l\binom{pm-1}{l} = \prod_{0<j\le l}\left(1 - p\frac{m}{j}\right) \equiv 1 - pm\sum_{0<j\le l}\frac{1}{j} \pmod{p^2}.$$

Combining this with (2.13) we then obtain (3.3). ■

Proof of Theorem 1.1. As $p-1$ is even, we have $B_{p-1}(1-x) = B_{p-1}(x)$.

(i) Let $l = [(n-\delta)/2]$ and $\varepsilon_n = (1 + (-1)^n)/2$. By Lemma 3.2,

$$\prod_{0<k\le l}(-1)^{[pk/n]}\binom{pm-1}{[pk/n]} \equiv 1 + pm\sum_{0<k\le l}\left(B_{p-1}\left(\left\{\frac{pk}{n}\right\}\right) - B_{p-1}\right) \pmod{p^2}.$$

Observe that

$$\begin{aligned}
2\sum_{0<k\le l}&\left(B_{p-1}\left(\left\{\frac{pk}{n}\right\}\right) - B_{p-1}\right) - \varepsilon_n(-1)^\delta\left(B_{p-1}\left(\frac{1}{2}\right) - B_{p-1}\right)\\
&= \sum_{0<k\le l}\left(B_{p-1}\left(\left\{\frac{pk}{n}\right\}\right) + B_{p-1}\left(\left\{\frac{p(n-k)}{n}\right\}\right) - 2B_{p-1}\right)\\
&\quad - \varepsilon_n(-1)^\delta\left(B_{p-1}\left(\left\{\frac{p}{2}\right\}\right) - B_{p-1}\right)\\
&= \sum_{k=0}^{n-1}\left(B_{p-1}\left(\left\{\frac{pk}{n}\right\}\right) - B_{p-1}\right) \equiv nq_p(n) \pmod{p}
\end{aligned}$$

where the last step is taken as in the proof of Proposition 2.2. By Corollary 2.1, $B_{p-1}(1/2) - B_{p-1} \equiv 2q_p(2) \pmod{p}$. Recall that $q_p(a) \equiv 2\left(\frac{a}{p}\right)\mathrm{eq}_p(a) \pmod{p}$ for any $a \in \mathbb{Z}$ with $(a, p) = 1$. So

$$\begin{aligned}
\sum_{0<k\le l}&\left(B_{p-1}\left(\left\{\frac{pk}{n}\right\}\right) - B_{p-1}\right)\\
&\equiv n\left(\frac{n}{p}\right)\mathrm{eq}_p(n) + \varepsilon_n(-1)^\delta 2\left(\frac{2}{p}\right)\mathrm{eq}_p(2) \pmod{p}.
\end{aligned}$$

By Lemma 3.1 and Gauss's Lemma,

$$(-1)^{\sum_{0<k\le l}[pk/n]} = (-1)^{l(p-1)/2 - \sum_{0<k<p/2}[nk/p]} = (-1)^{l(p-1)/2}\left(\frac{n}{p}\right)\left(\frac{2}{p}\right)^{n-1}.$$

Therefore

$$\begin{aligned}(-1)^{l(p-1)/2}\left(\frac{n}{p}\right)\left(\frac{2}{p}\right)^{n-1}&\prod_{0<k\le l}\binom{pm-1}{[pk/n]}\\ &=\prod_{0<k\le l}(-1)^{[pk/n]}\binom{pm-1}{[pk/n]}\\ &\equiv 1+pm\left(n\left(\frac{n}{p}\right)\mathrm{eq}_p(n)+\varepsilon_n(-1)^{\delta}2\left(\frac{2}{p}\right)\mathrm{eq}_p(2)\right)\pmod{p^2}\end{aligned}$$

and hence (1.3) follows.

(ii) Write S for the left hand side of (1.4) and set

$$S'=\sum_{r=0}^{n-1}(-1)^r B_{p-1}\left(\frac{r}{n}\right).$$

By Lemma 3.2,

$$\begin{aligned}S&\equiv\sum_{k=0}^{n-1}(-1)^{\{pk\}_n}\left(1+pm\left(B_{p-1}\left(\frac{\{pk\}_n}{n}\right)-B_{p-1}\right)\right)\\ &\equiv(1-pmB_{p-1})\Delta+pmS'\pmod{p^2}\end{aligned}$$

where

$$\{pk\}_n=n\left\{\frac{pk}{n}\right\}=pk-n\left[\frac{pk}{n}\right]\quad\text{and}\quad\Delta=\sum_{r=0}^{n-1}(-1)^r=\frac{1-(-1)^n}{2}.$$

If $2\nmid n$, then $S'=B_{p-1}$ since

$$(-1)^{n-r}B_{p-1}\left(\frac{n-r}{n}\right)=-(-1)^r B_{p-1}\left(\frac{r}{n}\right),$$

therefore $S\equiv 1\pmod{p^2}$. When $2\mid n$ we may apply Corollary 2.1. This concludes the proof. ∎

Proof of Theorem 1.2. Since $A\sim B$, by Theorem 2.1 and Proposition 2.1 we have

$$\sum_{s=1}^{k}\left(\left[\frac{x+pa_s}{n_s}\right]+\frac{1-p}{2}\right)=\sum_{t=1}^{l}\left(\left[\frac{x+pb_t}{m_t}\right]+\frac{1-p}{2}\right).$$

So (1.8) is equivalent to the following

$$\begin{aligned}P_A=\prod_{s=1}^{k}(-1)^{[(x+pa_s)/n_s]}&\binom{pN/n_s-1}{[(x+pa_s)/n_s]}\cdot\left(1-pN\sum_{s=1}^{k}\frac{q_p(n_s)}{n_s}\right)\\ \equiv P_B=\prod_{t=1}^{l}(-1)^{[(x+pb_t)/m_t]}&\binom{pN/m_t-1}{[(x+pb_t)/m_t]}\\ &\times\left(1-pN\sum_{t=1}^{l}\frac{q_p(m_t)}{m_t}\right)\pmod{p^2}.\end{aligned}$$

By (3.4) we have

$$\begin{aligned}
P_A &\equiv \prod_{s=1}^{k}\Big(1-p\frac{N}{n_s}\sum_{0<j\le[(x+pa_s)/n_s]}\frac{1}{j}\Big)\Big(1-pN\frac{q_p(n_s)}{n_s}\Big)\\
&\equiv \prod_{s=1}^{k}\Big(1-p\frac{N}{n_s}\Big(q_p(n_s)+\sum_{0<j\le[(x+pa_s)/n_s]}\frac{1}{j}\Big)\Big)\\
&\equiv \prod_{s=1}^{k}\Big(1-pNq\Big(\frac{x+pa_s}{n_s},n_s\Big)\Big)\\
&\equiv 1-pN\sum_{s=1}^{k}q\Big(\frac{x+pa_s}{n_s},n_s\Big) \pmod{p^2};
\end{aligned}$$

similarly

$$P_B \equiv 1-pN\sum_{t=1}^{l}q\Big(\frac{x+pb_t}{m_t},m_t\Big) \pmod{p^2}.$$

In view of Theorem 2.1 and Proposition 2.2, $P_A \equiv P_B \pmod{p^2}$. We are done. ∎

Acknowledgments. The author is indebted to Professor Andrew Granville for his comments, and to the referee for his suggestions.

References

[B] H. Bateman, *Higher Transcendental Functions*, A. Erdélyi *et al.* (eds.), Vol. I, McGraw-Hill, New York, 1953.

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

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

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, New York, 1990, 56–57, 235–236.

[J] M. Jenkins, *Proof of an Arithmetical Theorem leading, by means of Gauss' fourth demonstration of Legendre's law of reciprocity, to the extension of that law*, Proc. London Math. Soc. 2 (1867), 29–32.

[R] H. Rademacher, *Lectures on Elementary Number Theory*, Blaisdell, New York, 1964, Chapters 11 and 12.

[S1] Z. W. Sun, *Systems of congruences with multipliers*, J. Nanjing Univ. Math. Biquart. 6 (1989), no. 1, 124–133. MR 90m:11006; Zbl. M. 703.11002.

[S2] —, *Several results on systems of residue classes*, Adv. in Math. (China) 18 (1989), no. 2, 251–252.

[S3] —, *Covering the integers by arithmetic sequences II*, Trans. Amer. Math. Soc. 348 (1996), 4279–4320. MR 97c:11011.

[S4] Z. W. Sun, *Exact m-covers and the linear form $\sum_{s=1}^{k} x_s/n_s$*, Acta Arith. 81 (1997), 175–198. MR 98h:11019.

[S5] —, *On covering equivalence*, in: Analytic Number Theory, the joint Proceedings of the China–Japan Number Theory Conference (Beijing, 1999) and the RIMS Analytic Number Theory Conference (Kyoto, 1999), C. H. Jia and K. Matsumoto (eds.), Kluwer, to appear.

Department of Mathematics
Nanjing University
Nanjing 210093
People's Republic of China
E-mail: zwsun@nju.edu.cn

Received on 9.12.1999
and in revised form on 8.6.2000 (3723)