Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 123 (2007) 18–26
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Bernoulli numbers, Wolstenholme's theorem, and p^5 variations of Lucas' theorem ☆

Jianqiang Zhao

Department of Mathematics, Eckerd College, St. Petersburg, FL 33711, USA

Received 7 April 2003; revised 2 February 2006

Available online 30 June 2006

Communicated by Michael E. Pohst

Abstract

In this note we shall improve some congruences of G.S. Kazandzidis and D.F. Bailey to higher prime power moduli, by studying the relation between irregular pairs of the form $(p, p-3)$ and a refined version of Wolstenholme's theorem.

MSC: primary 11A07, 11Y40; secondary 11A41, 11M41

1. Introduction

Let $H_1(n)$ be the nth partial sum of the harmonic series. It is a classical result commonly attributed to Wolstenholme [5, p. 89] that for any prime $p \geqslant 5$

$$H_1(p-1) := \sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p^2}. \tag{1}$$

It is also known [10] that $H_1(p-1) \equiv 0 \pmod{p^3}$ if and only if $(p, p-3)$ is an irregular pair, namely, p divides the numerator of B_{p-3}. Here we define the Bernoulli numbers B_k by the

☆ Partially supported by NSF grant DMS0139813.
E-mail address: zhaoj@eckerd.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.05.005

Maclaurin series

$$\frac{x}{e^x-1}=\sum_{k=0}^{\infty}B_k\frac{x^k}{k!}.$$

There is another important equivalent statement of Wolstenholme's theorem by using combinatorics. Bailey [1] generalizes it to the following form.

Theorem 1.1. [1, Theorem 4] *Let n and r be non-negative integers and $p\geqslant 5$ be a prime. Then*

$$\binom{np}{rp}\equiv\binom{n}{r}\pmod{p^3},$$

where we set $\binom{n}{r}=0$ if $n<r$.

He further obtains the following variation of Lucas' theorem.

Theorem 1.2. [1, Theorem 5] *Let N, R, n and r be non-negative integers and $p\geqslant 5$ be a prime. Suppose $n,r<p$. Then*

$$\binom{Np^3+n}{Rp^3+r}\equiv\binom{N}{R}\binom{n}{r}\pmod{p^3}.$$

In late 1960's G.S. Kazandzidis worked on similar congruences. Define for any integer n and any positive integer r

$$\overline{\binom{n}{0}}=1,\qquad \overline{\binom{n}{r}}=\frac{n(n+1)\cdots(n+r-1)}{r!}.$$

Among many results he obtained in [8,9] the followings are particular relevant to our study

Theorem 1.3. [8, 2** on p. 10] *Let n be any integer and r be any positive integers and $p\geqslant 3$ be a prime. Then*

$$\overline{\binom{np}{rp}}\Big/\overline{\binom{n}{r}}\equiv\begin{cases}1-p^2nr(n+r)\pmod{p^3} & \text{if } p=3,\\ 1\pmod{p^3} & \text{if } p>3,\end{cases}\tag{2}$$

and

$$\binom{np}{rp}\Big/\binom{n}{r}\equiv\begin{cases}1-p^2nr(n-r)\pmod{p^3} & \text{if } p=3,\\ 1\pmod{p^3} & \text{if } p>3.\end{cases}\tag{3}$$

Here (2) *and* (3) *are equivalent.*

In this short note we will refine the above results for primes $p>5$ by using higher prime power modulus (see Theorem 3.2). This is best possible in the sense that the result would be wrong if we allowed $p=5$. Note that in [9] Kazandzidis obtains an improved version of his

congruences of Theorem 1.3 by replacing the modulus by $p^3\bar{p}\{nr(n-r)\}$, where $\bar{p}\{N\}$ denotes the highest power of the prime p that divides N. This improvement does not follow from our result in this paper. However, it does not imply ours either.

In the last section of this paper we provide an interesting congruence involving Bernoulli numbers of the form B_{p-3} for odd primes p.

2. Preliminaries and some notation

Define the Euler–Zagier multiple zeta functions of depth d by

$$\zeta(s_1,\dots,s_d)=\sum_{0<k_1<\cdots<k_d} k_1^{-s_1}\cdots k_d^{-s_d} \tag{4}$$

for complex variables $s_1,\dots,s_d$ satisfying $\mathrm{Re}(s_j)+\cdots+\mathrm{Re}(s_d)>d-j+1$ for all $j=1,\dots,d$. The special values of multiple zeta functions at positive integers have significant arithmetic and algebraic meanings, whose defining series (4) will be called *MZV series*, and whose nth partial sum is

$$H(s_1,\dots,s_d;n):=\sum_{1\leqslant k_1<\cdots<k_d\leqslant n} k_1^{-s_1}\cdots k_d^{-s_d},\quad n\in\mathbb{Z}_{\geqslant 0}. \tag{5}$$

Note that partial sums exist even for divergent MZV $\zeta(\dots,1)$ such as the harmonic series $\zeta(1)$. When an ordered set $(e_1,\dots,e_t)$ is repeated d times we abbreviate it as $\{e_1,\dots,e_t\}^d$. From the definitions (4) and (5) one derives easily the so-called shuffle relations. For example,

$$\zeta(s)\zeta(t)=\zeta(t,s)+\zeta(t+s)+\zeta(s,t)$$

because

$$\sum_{k>0}\cdot\sum_{l>0}=\sum_{k>l>0}+\sum_{k=l>0}+\sum_{0<k<l}.$$

Similarly, one has

$$H(s;n)H(t;n)=H(t,s;n)+H(t+s;n)+H(s,t;n). \tag{6}$$

Recall that Stirling numbers $S(n,j)$ of the first kind are defined by the expansion

$$f_n(x)=x(x-1)(x-2)\cdots(x-n+1)=\sum_{j=1}^{n}(-1)^{n-j}S(n,j)x^j. \tag{7}$$

These numbers are related to the partial sums of nested harmonic series:

$$S(n,j)=(n-1)!H\big(\{1\}^{j-1};n-1\big),\quad \text{for } j=1,\dots,n. \tag{8}$$

For example, $S(n,n)=1$, $S(n,n-1)=n(n-1)/2$, and $S(n,1)=(n-1)!$. In particular, if $n=p$ is a prime we then have

$$f_p(x)=(p-1)!x\big(1-H(1;p-1)x+H(1,1;p-1)x^2-\cdots+x^{p-1}\big).$$

Comparing $f_p(p) = p!$ we recover the Wolstenholme theorem.

One last thing we need in this note is the following generalization of (1).

Lemma 2.1. [11, Theorem 2.13] *Let s and d be two positive integers. Let p be an odd prime such that $p \geqslant sd + 3$. Then*

$$H\big(\{s\}^d; p-1\big) \equiv \begin{cases} 0 \pmod{p^2} & \text{if } 2 \nmid sd, \\ 0 \pmod{p} & \text{if } 2 \mid sd. \end{cases}$$

3. Main results

Our first result improves on Theorem 1.1 of Bailey and Theorem 1.3 of Kazandzidis simultaneously for all primes greater than 5.

Definition 3.1. For any prime $p \geqslant 5$ by Wostenholme's theorem (1) we define $w_p < p^2$ to be the unique non-negative integer such that $w_p \equiv H_1(p-1)/p^2 \pmod{p^2}$. It is a well-known fact that (see for e.g., [4])

$$w_p \equiv -\frac{1}{3} B_{p-3} \pmod{p}. \tag{9}$$

Theorem 3.2. *Let n and r be non-negative integers and $p \geqslant 7$ be a prime. Then*

$$\binom{np}{rp} \Big/ \binom{n}{r} \equiv 1 + w_p nr(n-r)p^3 \pmod{p^5}. \tag{10}$$

Moreover,

$$\binom{np}{rp} \Big/ \binom{n}{r} \equiv 1 \pmod{p^4} \tag{11}$$

for all n, r if and only if p divides the numerator of B_{p-3}.

Remark 3.3. When $p = 5$ Theorem 3.2 does not hold. Indeed, it is easy to see that $H_1(4) = 25/12$ so $w_5 = 23$. Now take $n = 4$ and $r = 1$. Then

$$\binom{4\cdot 5}{5} \Big/ \binom{4}{1} \equiv 751 \not\equiv 1 + 23 \cdot 4 \cdot 1 \cdot 3 \cdot 5^3 \equiv 126 \pmod{5^5}.$$

Proof of Theorem 3.2. Clearly we may assume $n > r$. To save space we write $H_k = H(\{1\}^k; p-1)$ throughout this proof. By Eq. (7) we have

$$\binom{np}{rp} = \frac{\prod_{j=n-r+1}^{n} f_p(jp)}{\prod_{l=1}^{r} f_p(lp)}.$$

By relation (8) and Lemma 2.1 we have

$$\binom{np}{rp} \Big/ \binom{n}{r} \equiv \frac{\prod_{j=n-r+1}^{n} (1 - jpH_1 + j^2p^2H_2)}{\prod_{l=1}^{r} (1 - lpH_1 + l^2p^2H_2)} \pmod{p^5}. \tag{12}$$

Now it follows quickly from (1) and the shuffle relation (6) that

$$2H_2 + H(2; p-1) = H_1^2 \equiv 0 \pmod{p^4}. \tag{13}$$

By substitution $k \to p-k$ we further can see that

$$\begin{aligned} 2H_1 &= \sum_{k=1}^{p-1} \frac{p}{k(p-k)} \equiv -\sum_{k=1}^{p-1} \frac{p}{k^2}\left(1 + \frac{p}{k} + \frac{p^2}{k^2}\right) \pmod{p^4} \\ &\equiv -\big(pH(2; p-1) + p^2 H(3; p-1) + p^3 H(4; p-1)\big) \pmod{p^4} \\ &\equiv -pH(2; p-1) \pmod{p^4} \\ &\equiv 2pH_2 \pmod{p^4}. \end{aligned} \tag{14}$$

Congruence (14) is obtained by Lemma 2.1 (so we indeed need the condition $p \geqslant 7$) while the last step follows from (13). Therefore by (1) congruence (12) is reduced to

$$\begin{aligned} \binom{np}{rp} \Big/ \binom{n}{r} &\equiv 1 + \sum_{j=n-r+1}^{n} (j^2 - j)pH_1 - \sum_{l=1}^{r} (l^2 - l)pH_1 \pmod{p^5} \\ &\equiv 1 + w_p nr(n-r)p^3 \pmod{p^5}. \end{aligned}$$

This proves congruence (10). The last statement of the theorem follows from (9) immediately. □

By induction on the exponent the following corollary is obvious.

Corollary 3.4. *Let $p \geqslant 7$ be a prime and let r and n be two non-negative integers. Then for any exponent $e \geqslant 1$ we have*

$$\binom{np^e}{rp^e} \Big/ \binom{n}{r} \equiv 1 + w_p nr(n-r)p^3 \pmod{p^5}.$$

Next we consider a refined version of Theorem 1.2 of Bailey.

Theorem 3.5. *Let N, R, n and r be non-negative integers and $p \geqslant 7$ be a prime. If $r \leqslant n < p$ then*

$$\binom{Np^3 + n}{Rp^3 + r} \Big/ \left[\binom{N}{R}\binom{n}{r}\right] \equiv 1 + c(N, R, n, r; p)p^3 \pmod{p^5}, \tag{15}$$

where $c(N, R, n, r; p) = H_1(n)N - H_1(r)R + (w_p NR - H_1(n-r))(N-R)$. If $n < r < p$ then

$$\binom{Np^3 + n}{Rp^3 + r} \Big/ \binom{N}{R} \equiv (-1)^{r-n+1} \frac{N-R}{n} \binom{r-1}{n}^{-1} p^3 \pmod{p^5}. \tag{16}$$

Proof. Clearly we can assume that $N \geqslant R$. Observe that we have a variant of $f_n(x)$ defined by (7):

$$\begin{aligned} F_n(x) &= (-1)^{n+1} f_{n+1}(-x)/x = (x+1)(x+2)\cdots(x+n) \\ &= n!\big(1 + H(1;n)x + H(1,1;n)x^2 + \cdots\big). \end{aligned}$$

First, let $r \leqslant n < p$. Then by straightforward expansion we have

$$\begin{aligned} \binom{Np^3+n}{Rp^3+r}\Big/\left[\binom{N}{R}\binom{n}{r}\right] &= \left[\binom{Np^3}{Rp^3}\Big/\binom{N}{R}\right]\frac{r!(n-r)!\cdot\prod_{i=1}^{n}(Np^3+i)/n!}{\prod_{i=1}^{r}(Rp^3+i)\prod_{i=1}^{n-r}((N-R)p^3+i)} \\ &= \left[\binom{Np^3}{Rp^3}\Big/\binom{N}{R}\right]\frac{F_n(Np^3)}{F_r(Rp^3)F_{n-r}((N-R)p^3)} \\ &\equiv \frac{(1+H_1(n)Np^3)(1+w_pNR(N-R)p^3)}{(1+H_1(r)Rp^3)(1+H_1(n-r)(N-R)p^3)} \pmod{p^5} \end{aligned}$$

by Corollary 3.4 and the fact that $H_1(m)$ is p-integral if $m < p$. Congruence (15) follows immediately. □

Example 3.6. Take $p = 7$. Then the following congruence is exact (and the term $c(\cdots)p^3$ is not needed):

$$\binom{4\cdot 7^3+5}{2\cdot 7^3+2} \equiv \binom{4}{2}\binom{5}{2} \pmod{7^5}.$$

Using GP Pari and taking $1 \leqslant N, R, n, r \leqslant 6$ we find the complete list of nontrivial (N, R, n, r) (i.e., $N \neq R$ or $n \neq r$) for which this type of congruence holds when $p = 7$: $(4,2,5,2)$, $(4,2,5,3)$, $(5,2,6,1)$, $(4,2,6,3)$, $(5,1,6,3)$, $(5,4,6,3)$, $(5,3,6,5)$. We believe there are always such nontrivial congruences for every prime $p \geqslant 7$.

Remark 3.7. (1) If $p = 5$ then congruence (15) of Theorem 3.5 is not true anymore. For example, take $N = 3$, $n = 4$, $R = r = 1$. Then $c(3,1,4,1;5) = 1675/12$. So

$$\binom{3\cdot 5^3+4}{5^3+1}\Big/\left[\binom{3}{1}\binom{4}{1}\right] \equiv 2501 \not\equiv 1 + c(3,1,4,1;5)5^3 \equiv 1 \pmod{5^5}.$$

(2) If $p = 5$ then congruence (16) of Theorem 3.5 still holds for all possible $N, R < 5^5$ and $n < r < 5$. I believe this is true for all other N and R.

4. An interesting sum related to $\zeta(1,2)$

The last result of this note is related to the above theme and has some independent interest. We discovered this when trying to prove Theorem 3.2 in the special case $r = 1$ following Gardiner's suggestion in [3]. We failed but obtained this unexpected byproduct.

Proposition 4.1. *Suppose p is an odd prime. Then*

$$2H(2,1;p-1) \equiv -2H(1,2;p-1) \equiv \sum_{\substack{i+j+k=p \\ i,j,k>0}} \frac{1}{ijk} \pmod{p}.$$

Proof. By the shuffle relation (6) and Lemma 2.1 we have

$$H(2,1;p-1) + H(1,2;p-1) = H(1;p-1)H(2;p-1) - H(3;p-1) \equiv 0 \pmod{p}.$$

So the first congruence is obvious. Let us prove the second.

The cases $p = 3$ and 5 can be checked easily:

$$2H(1,2;2) + \sum_{\substack{i+j+k=3 \\ i,j,k>0}} \frac{1}{ijk} = \frac{1}{2} + 1 = \frac{3}{2} \equiv 0 \pmod{3},$$

$$2H(1,2;4) + \sum_{\substack{i+j+k=5 \\ i,j,k>0}} \frac{1}{ijk} = \frac{17}{16} + \frac{7}{4} = \frac{45}{16} \equiv 0 \pmod{5}.$$

Suppose now $p \geqslant 7$. Let us go through Gardiner's proof of [3, Theorem 1]. Let $n > 3$ be a positive integer (we will take $n = p - 1$ later). Combinatorial consideration leads us to

$$\begin{aligned} 3\binom{np}{p} &= \sum_{i_1+\cdots+i_n=p} \binom{p}{i_1}\cdots\binom{p}{i_n} \\ &\equiv n + \binom{n}{2} \sum_{\substack{i+j=p \\ i,j>0}} \binom{p}{i}\binom{p}{j} + \binom{n}{3} \sum_{\substack{i+j+k=p \\ i,j,k>0}} \binom{p}{i}\binom{p}{j}\binom{p}{k} \pmod{p^4} \qquad (17) \\ &\equiv n + \binom{n}{2}X + \binom{n}{3}Y \pmod{p^4}, \end{aligned}$$

where X and Y are given by the two sums in (17), respectively. Recall from (7) and (8)

$$f_i(x) = x(x-1)\cdots(x-i+1) = (i-1)!\sum_{j=1}^{n}(-1)^{i-j}H\big(\{1\}^{j-1};i-1\big)x^j.$$

Hence

$$\begin{aligned} X = \sum_{i=1}^{p-1}\left(\frac{f_i(p)}{i!}\right)^2 &= \sum_{i=1}^{p-1}\frac{p^2}{i^2}\left(\sum_{j=1}^{i}(-1)^{i-j}H\big(\{1\}^{j-1};i-1\big)p^{j-1}\right)^2 \\ &\equiv \sum_{i=1}^{p-1}\frac{p^2}{i^2}\big(1-2H(1;i-1)p\big) \pmod{p^4} \\ &\equiv p^2H(2;p-1) - 2p^3H(1,2;p-1) \pmod{p^4}. \end{aligned}$$

As for Y we have $Y = 0$ if $n = 2$. If $n \geqslant 3$ then

$$Y = \sum_{\substack{i+j+k=p \\ i,j,k>0}} \frac{1}{i!j!k!} \prod_{\alpha=i,j,k} \left(\sum_{l=1}^{\alpha} (-1)^{l-\alpha} S(\alpha, l) p^l \right) \equiv \sum_{\substack{i+j+k=p \\ i,j,k>0}} \frac{p^3}{ijk} \pmod{p^4}.$$

Putting every thing together with $n = p - 1$, comparing to (10) with $r = 1$, using the fact $2H(1; p-1) \equiv -pH(2; p-1) \pmod{p^4}$ from (14), and canceling the factor $n(n-1)/2$, we arrive at

$$-np^2 H(2; p-1) \equiv p^2 H(2; p-1) - 2p^3 H(1, 2; p-1) + \frac{n-2}{3} \sum_{\substack{i+j+k=p \\ i,j,k>0}} \frac{p^3}{ijk} \pmod{p^4}.$$

With $n = p - 1$ this simplifies to

$$2H(1, 2; p-1) - \frac{p-3}{3} \sum_{\substack{i+j+k=p \\ i,j,k>0}} \frac{1}{ijk} \equiv H(2; p-1) \equiv 0 \pmod{p},$$

whence the second congruence in the proposition. □

Combining Proposition 4.1 with [11, Theorem 3.1] we find the following corollary.

Corollary 4.2. *For any prime* $p \geqslant 5$

$$\sum_{\substack{i+j+k=p \\ i,j,k>0}} \frac{1}{ijk} \equiv -2B_{p-3} \pmod{p}.$$

Remark 4.3. (1) We know that among all the primes p less than 12 million p divides the numerator of B_{p-3} only for $p = 16\,843$ and $p = 2\,124\,679$ (see [2]). However, we believe there exist infinitely many such primes.

(2) In a recent paper Ji provides a proof of Corollary 4.2 without using partial sums of MZV series (see [6]). In more recent preprints he [7] and independently, Zhou and Cai [12], generalize this to sums of arbitrary lengths: let $p \geqslant 5$ be a prime and $n \leqslant p-2$ a positive integer, then

$$\sum_{\substack{l_1+l_2+\cdots+l_n=p \\ l_1,\ldots,l_n>0}} \frac{1}{l_1 l_2 \cdots l_n} \equiv \begin{cases} -(n-1)! B_{p-n} \pmod{p} & \text{if } 2 \nmid n, \\ -\frac{n! np}{2(n+1)} B_{p-n-1} \pmod{p^2} & \text{if } 2 \mid n. \end{cases}$$

Acknowledgment

The author thanks the referee for pointing out Kazandzidis' work [8,9] and many other valuable comments which make this note more readable.

References

[1] D.F. Bailey, Two p^3 variations of Lucas' theorem, J. Number Theory 35 (2) (1990) 208–215, MR: 91f:11008.
[2] J.P. Buhler, R.E. Crandall, R. Ernvall, T. Metsänkylä, M.A. Shokrollahi, Primes and cyclotomic invariants to 12 million, in: Computational Algebra and Number Theory, Milwaukee, WI, 1996, J. Symbolic Comput. 31 (2001) 89–96, MR: 2001m:11220.
[3] A. Gardiner, Four problems on prime power divisibility, Amer. Math. Monthly 95 (1988) 926–931.
[4] J.W.L. Glaisher, On the residues of the sums of the inverse powers of numbers in arithmetical progression, Q. J. Math. 32 (1900) 271–288.
[5] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Clarendon, Oxford, 1980.
[6] Chun-Gang Ji, A simple proof of a curious congruence by Zhao, Proc. Amer. Math. Soc. 133 (2005) 3469–3472.
[7] Chun-Gang Ji, Generalization of Wolstenholme's theorem, preprint.
[8] G.S. Kazandzidis, Congruences on the binomial coefficients, Bull. Soc. Math. Grèce (N.S.) 9 (fasc. 1) (1968) 1–12, MR: 42#182.
[9] G.S. Kazandzidis, On congruences in number-theory, Bull. Soc. Math. Grèce (N.S.) 10 (fasc. 1) (1969) 35–40, MR: 43#4753.
[10] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Ann. of Math. (2) 39 (1938) 350–360.
[11] J. Zhao, Partial sums of multiple zeta value series I: Generalizations of Wolstenholme's theorem, http://xxx.lanl.gov/abs/math.NT/0301252, v1.
[12] X. Zhou, T. Cai, A generalization of a curious congruence by Zhao, Proc. Amer. Math. Soc., in press.