

## THE UNIVERSAL KUMMER CONGRUENCES

SHAOFANG HONG , JIANRONG ZHAO and WEI ZHAO

(Received 28 June 2010; accepted 29 June 2012; first published online 22 March 2013)

Communicated by I. E. Shparlinski

Dedicated to Professor Qi Sun on the occasion of his 75th Birthday

### Abstract

Let  $p$  be a prime. In this paper, we present a detailed  $p$ -adic analysis on factorials and double factorials and their congruences. We give good bounds for the  $p$ -adic sizes of the coefficients of the divided universal Bernoulli number  $B_n/n$  when  $n$  is divisible by  $p - 1$ . Using these, we then establish the universal Kummer congruences modulo powers of a prime  $p$  for the divided universal Bernoulli numbers  $B_n/n$  when  $n$  is divisible by  $p - 1$ .

*2010 Mathematics subject classification:* primary 11D79; secondary 11B68, 11A07.

*Keywords and phrases:* universal Bernoulli number, universal Kummer congruence, double factorial,  $p$ -adic valuation, reduced partition.

### 1. Introduction

Bernoulli numbers occur in many parts of number theory. Let  $n \geq 0$  be an integer. Then the  $n$ th Bernoulli number is defined by the following formula:

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n. \quad (1.1)$$

From (1.1) one can see that  $B_1 = -1/2$  and  $B_n = 0$  for all odd  $n > 1$ . The first few values for even  $n$  are:  $B_0 = 1$ ,  $B_2 = 1/6$ ,  $B_4 = -1/30$ ,  $B_6 = 1/42$ , etc. The periodic behavior of the divided Bernoulli numbers  $B_n/n$  is closely related to the existence of a  $p$ -adic zeta function [17]. The classical Kummer congruences [14] concern the congruence relations among the divided Bernoulli numbers  $B_n/n$ . In fact, they state that if  $p$  is a prime and  $(p - 1) \nmid n$  and  $n \equiv m \pmod{p - 1}$ , then  $B_n/n \equiv B_m/m \pmod{p}$ . One can

The first author was supported in part by the National Science Foundation of China Grant no. 10971145 and by the PhD Programs Foundation of Ministry of Education of China Grant no. 20100181110073

© 2013 Australian Mathematical Publishing Association Inc. 1446-7887/2013 \$16.00

prove this congruence by means of  $p$ -adic measures and  $p$ -adic integration [21, 22]. In [4], Baker *et al.* established some global-local Kummer congruences. There are also many other elegant and useful congruences, such as Wilson's theorem [2, 15], Fermat's little theorem [13, 15], Wolstenholme's theorem [23], Lucas' congruence [19] and Glaisher's congruence [8–10]. In this paper, we will mainly be concerned with the universal Kummer congruences.

In 1989, Clarke [5] introduced the concept of universal Bernoulli numbers. Assume that  $c_1, c_2, \dots$  are indeterminates over  $\mathbf{Q}$ . Then let  $F(t) = t + c_1 t^2/2 + c_2 t^3/3 + \dots$  and let  $G(t) = F^{-1}(t)$  be the compositional formal power series inverse of  $F(t)$ , namely  $F(G(t)) = G(F(t)) = t$ . The *universal Bernoulli numbers*  $\hat{B}_n$  are defined by

$$\frac{t}{G(t)} = \sum_{n=0}^{\infty} \frac{\hat{B}_n}{n!} t^n.$$

Obviously we have  $\hat{B}_n \in \mathbf{Q}[c_1, c_2, \dots, c_n]$ . Actually  $\hat{B}_n$  is a nontrivial  $\mathbf{Q}$ -linear combination of all the monomials of weight  $n$ , where  $c_i$  has weight  $i$ . So  $\hat{B}_n$  is the sum of  $p(n)$  monomials, where  $p(n)$  is the partition function. Recently, Tempesta [20] introduced the universal higher-order Bernoulli polynomials and universal Bernoulli  $\chi$ -numbers.

Substituting  $c_i = (-1)^i$ , we get  $F(t) = \log(1+t)$  so that  $G(t) = e^t - 1$  and we obtain the classical Bernoulli numbers  $B_n = \hat{B}_n$ . Miller [16] investigated the specialization where  $c_i$  is the equivalence class of the complex projective space and proved that for this specialization, if  $k$  is odd and  $k \neq 1$ , then  $\hat{B}_k/k \in L$ , where  $L$  is the *Lazard ring*, a subring of  $\mathbf{Q}[c_1, c_2, \dots]$ . Clarke [5] showed that the divided universal Bernoulli number  $\hat{B}_n/n$  is  $p$ -integral if  $(p-1) \nmid n$  which forms part of his universal von Staudt theorem. Adelberg [1] set up the universal Kummer congruences modulo a prime  $p$  for the divided universal Bernoulli numbers  $\hat{B}_n/n$  when  $(p-1) \nmid n$ . Soon thereafter, Adelberg [2] obtained the universal Kummer congruences modulo powers of a prime  $p$  for the case  $(p-1) \nmid n$ . Adelberg *et al.* [3] established the universal Kummer congruences modulo a prime  $p$  for the divided universal Bernoulli numbers when  $(p-1) \mid n$ . Furthermore, Adelberg *et al.* [3] gave a simple proof to Clarke's 1989 universal von Staudt theorem [5] which generalized the theorems of Dibag [7], Ray [18], Katz [12] and Hurwitz [11]. It is natural to ask the question of establishing the universal Kummer congruences modulo powers of a prime  $p$  for the divided universal Bernoulli numbers when  $(p-1) \mid n$ .

In the present paper, our main goal is to investigate the above problem. We will exploit the universal Kummer congruence modulo powers of a prime  $p$  for the divided universal Bernoulli numbers for the remaining case  $(p-1) \mid n$ . This is divided into two subcases: the even prime 2 and odd primes  $p$  such that  $(p-1) \mid n$ . For this purpose, we need to estimate  $p$ -adic valuations of the coefficients of the divided universal Bernoulli number  $\hat{B}_n/n$  when  $n$  is divisible by  $p-1$ . The paper is organized as follows. In Section 2 we present notations and some preliminary results. In Section 3 we establish the universal Kummer congruences modulo powers of odd primes  $p$  when  $(p-1) \mid n$ .

Then, in Section 4, we treat the even prime  $p = 2$  case. We provide a detailed 2-adic analysis to many kinds of factorials and double factorials. Finally, in Section 5, we set up the universal Kummer congruences modulo powers of 2. Our result extends and strengthens the Adelberg–Hong–Ren theorem. It also extends Clarke’s theorem and complements Adelberg’s modulo prime powers result.

### 2. Preliminaries

If  $u = (u_1, u_2, \dots) \in \mathbf{N}^\infty$  with  $u_i = 0$  if  $i$  is sufficiently large and  $w(u) := \sum iu_i$ , we identify  $u$  with a partition of  $w(u)$ , where  $u_i$  is the number of occurrences of part  $i$  in the partition. If  $d(u) := \sum u_i$ , then  $d(u)$  is the number of parts in the partition. We call  $w(u)$  the *weight* of  $u$  and  $d(u)$  the *degree* of  $u$ . If  $u_i = 0$  for  $i > n$ , we write  $u \in \mathbf{N}^n$ . Let  $k \geq 1$  and  $l \geq 1$  be integers.

As usual, we let  $v = v_p$  be the *normalized  $p$ -adic valuation* of  $\mathbf{Q}$ , that is,  $v(a) = b$  if  $p^b \mid a$  and  $p^{b+1} \nmid a$ . We can extend  $v$  to  $\mathbf{Q}[c_1, c_2, \dots]$  by  $v(\sum a_u c^u) = \min\{v(a_u)\}$  when  $u = (u_1, \dots, u_n) \in \mathbf{N}^n$  and  $c^u = c_1^{u_1} \dots c_n^{u_n}$ . By the Lagrange inversion [5],

$$\frac{\hat{B}_n}{n} = \sum_{w(u)=n} \tau_u c^u, \tag{2.1}$$

where  $u = (u_1, \dots, u_n) \in \mathbf{N}^n$ ,  $d = d(u)$ ,  $c^u = c_1^{u_1} \dots c_n^{u_n}$ ,

$$\gamma_u = 2^{u_1} \dots (n + 1)^{u_n} u_1! \dots u_n!$$

and

$$\tau_u = (-1)^{d-1} \frac{(n + d - 2)!}{\gamma_u}.$$

For any positive odd integer  $a$ , we define the *double factorial*  $a!!$  of  $a$  by  $a!! = \prod_{1 \leq k \leq a, (2,k)=1} k$ . That is,  $a!! = a \cdot (a - 2) \cdot \dots \cdot 3 \cdot 1$ . For a real number  $x$ , define  $\lceil x \rceil$  to be the least integer greater than  $x$  and  $\lfloor x \rfloor$  to be the greatest integer less than  $x$ . Then  $\lceil x \rceil + \lceil y \rceil \geq \lceil x + y \rceil$ ,  $\lceil n + x \rceil = n + \lceil x \rceil$ ,  $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$  and  $\lfloor n + x \rfloor = n + \lfloor x \rfloor$  for any real numbers  $x$  and  $y$  and any integer  $n$ .

We will freely use the standard results listed in the following Lemma 2.1.

**LEMMA 2.1.** *We have*

$$v((ab)!) \geq v(a!) + v(b!), \tag{2.2}$$

$$v((lp)!) = l + v(l!).$$

Moreover,

$$v((lp^t)!) = l(p^t - 1)/(p - 1) + v(l!), \tag{2.3}$$

$$v(a!) = v(\lfloor a/p \rfloor p!) = (a - s(a))/(p - 1), \tag{2.4}$$

where  $s(a) := \sum_{i=0}^t a_i$  is the base  $p$  digit sum if  $a = \sum_{i=0}^t a_i p^i$  with digits  $0 \leq a_i \leq p - 1$ , and

$$v(a!) \leq (a - 1)/(p - 1) \quad \text{if } a > 0. \tag{2.5}$$

LEMMA 2.2 [2]. *If  $p$  is an odd prime and  $N = v(l)$ , then*

$$(lp)!/(l!p^l) \equiv (-1)^l \pmod{p^{N+1}}.$$

LEMMA 2.3 [2]. *We have  $v((\sum h_j p^j)!) \geq \sum(jh_j + v(h_j!))$ .*

LEMMA 2.4 [2]. *If  $p$  is an odd prime and  $0 < k \leq p$ , then*

$$v(a!) \geq v(a + k)$$

*unless  $a = p - k$ , in which case  $v(a!) = v(a + k) - 1$ .*

Clarke [5] proved some congruences about factorials. Clarke and Jones [6] obtained some stronger congruences about factorials while Adelberg *et al.* [3] strengthened Clarke’s congruence for the  $p = 2$  case. But for our purpose, we need the following result due to Adelberg [2].

LEMMA 2.5 [2]. *Let  $v(l) = N$ . Then:*

- (i)  $((l + q)p)!/((l + q)!p^{l+q}) \equiv (-1)^l \cdot (qp)!/(q!p^q) \pmod{p^{N+1}}$ ;
- (ii)  $((l + q)p + a)!/((l + q)!p^{l+q}) \equiv (-1)^l \cdot (qp + a)!/(q!p^q) \pmod{p^{N+1}}$ ;
- (iii) *if  $a \geq ep$ , then the congruence (ii) holds  $\pmod{p^{N+e}}$ ;*
- (iv) *if  $a \geq (e + 1)p$ , then*

$$((l + q)p + a)!/((l + q)!p^{l+q+e}) \equiv (-1)^l \cdot (qp + a)!/(q!p^{q+e}) \pmod{p^{N+1}}.$$

### 3. Universal Kummer congruences modulo odd prime powers

In the present section, we treat the odd prime case. We set up the universal Kummer congruences modulo odd prime powers. We begin with the following concept. Note that it is different from [2, Definition 4.1].

DEFINITION 3.1. A partition  $u$  is called *reduced* if there is at most one part  $g \in \mathbf{N}$  such that  $g \neq p^\alpha - 1$ ,  $u_g = 1$  and if  $i \neq g$  and  $u_i \neq 0$ , then  $i = p^\alpha - 1$ .

LEMMA 3.2. *Assume that  $n = (m + i)p - i = i(p - 1) + mp$  where  $i \geq 0$ . Let  $w(u) = n$  and suppose that  $d(u) \leq i + 1$ . Then there exists a reduced partition  $u'$  such that  $w(u') = n$ ,  $d(u') \leq i + 1$  and  $v(\tau_u) \geq v(\tau_{u'})$ .*

PROOF. We first define a partition  $u''$ : if  $t \neq p^\alpha - 1$ , then  $u''_t := 0$ ; if  $t = p^\alpha - 1$ , then

$$u''_t = u''_{p^\alpha - 1} := \sum_{\varepsilon \in \mathbf{Z}^+, p \nmid \varepsilon} u_{\varepsilon p^\alpha - 1} + \delta(\alpha) \sum_{u_j \geq p, p \nmid (j+1)} \left( \left\lfloor \frac{u_j}{p-1} \right\rfloor - 1 \right),$$

where  $\delta(\alpha) = 1$  for  $\alpha = 1$  and  $\delta(\alpha) = 0$  for  $\alpha \geq 2$ . In fact, we construct  $u''$  as follows.

(i) If  $u_t \neq 0$  with  $t = \varepsilon p^\alpha - 1$  and  $p \nmid \varepsilon$  and  $\varepsilon > 1$ , let  $u''_t = 0$  and  $u''_k = u_k + u_t$  where  $k = p^\alpha - 1$ , that is, transfer  $u_t$  to part  $p^\alpha - 1$ .

(ii) If  $u_t \geq p$ , where  $p \nmid (t + 1)$ , let  $u''_t = 0$  and  $u''_{p-1} = u_{p-1} + \lceil u_t / (p - 1) \rceil - 1$ , that is, transfer to part  $p - 1$ .

(iii) If  $0 < u_t < p$  and  $p \nmid (t + 1)$ , let  $u'_t = 0$ , that is, delete part  $t$  from the partition. The partition  $u'_t$  is formed by considering all parts, and should be thought of as loading the parts where  $i = p^\alpha - 1$ . All other parts of  $u$  where (i)–(iii) do not apply are unchanged. The partition  $u'_t$  can be constructed from  $u$  one part at a time or all at once.

Clearly  $w(u'') \leq n$ , and if  $u_i \neq 0$  then  $i = p^\alpha - 1$ . Observe that  $v(\gamma''_u) \geq v(\gamma_u)$  by (2.3) and (2.5), and that  $d(u'') = d(u)$  if all modifications are of type (i), and otherwise  $d(u'') < d(u)$ .

Next let  $g = n - w(u'') \geq 0$ . If  $g = 0$ , let  $u' = u''$ . Then  $u'$  is just what we need.

If  $g > 0$ , let  $u'_g = u''_g + 1$  and  $u'_j = u''_j$  if  $j \neq g$ . Then  $u'$  is reduced,  $w(u') = n$ ,  $d' = d(u') = d(u'') + 1$  and  $v(\gamma_{u'}) \geq v(\gamma_{u''}) \geq v(\gamma_u)$ . If  $d(u'') < d(u)$ , then  $d(u') \leq d(u) \leq i + 1$ . Hence  $v(\tau_u) \geq v(\tau_{u'})$ . Finally, assume that  $d(u'') = d(u)$ . In this case all modifications are of type (i), so

$$n = \sum iu_i = \sum (\varepsilon p^\alpha - 1)u_{\varepsilon p^\alpha - 1}$$

and  $d = \sum u_{\varepsilon p^\alpha - 1}$ . But  $n = (m + i)p - i$ , thus  $i \equiv \sum u_{\varepsilon p^\alpha - 1} = d(u) \pmod p$ . Since  $1 \leq d(u) \leq i + 1$ , it follows that  $d(u) \leq i$  and  $d(u') = d(u) + 1 \leq i + 1$ . Also  $n + d - 2 = \sum \varepsilon p^\alpha u_{\varepsilon p^\alpha - 1} - 2$ . Hence  $v((n + d - 2)!) = v((n + d' - 2)!) by (2.4), which means that  $v(\tau_u) \geq v(\tau_{u'})$ . The proof is complete.  $\square$$

**LEMMA 3.3.** *Let  $n = (m + i)p - i$  with  $m = s(p - 1)$ . Let  $u$  be reduced, with  $w(u) = n$  and  $d \leq i + 1$ . Then  $v(\tau_u) \geq s(p - 2) - 1$ .*

**PROOF.** Let  $h_j = u_{p^j - 1}$  with  $j \geq 1$ . Consider the following cases:

*Case 1.* If  $u_t \neq 0$ , then  $t = p^\alpha - 1$ . In this case,  $d = \sum_{j \geq 1} h_j$  and

$$n = \sum_{j \geq 1} h_j(p^j - 1) = (m + i)p - i.$$

Then  $i \equiv \sum_{j \geq 1} h_j = d \pmod p$ . Since  $d \leq i + 1$ , we may let  $i = d + kp$  with  $k \geq 0$ . Then

$$n + d - 2 = \sum_{j \geq 1} h_j p^j - 2 = (m + i)p - i + d - 2 = (m + i - k)p - 2.$$

This implies that  $k = m + i - \sum_{j \geq 1} h_j p^{j-1}$ . It is easy to see that  $v(\gamma_u) = \sum_{j \geq 1} (jh_j + v(h_j!))$ . Hence by Lemma 2.3,

$$\begin{aligned} v(\tau_u) &= v(((m + i - k)p - 2)!) - \sum_{j \geq 1} (jh_j + v(h_j!)) \\ &= m + i - k - 1 + v((m + i - k - 1)!) - \sum_{j \geq 1} (jh_j + v(h_j!)) \\ &= m + i - k - 1 + v\left(\left(\sum_{j \geq 1} h_j p^{j-1} - 1\right)!\right) - \sum_{j \geq 1} ((j - 1)h_j + v(h_j!)) - d \\ &= m - 1 + k(p - 1) + \beta, \end{aligned} \tag{3.1}$$

where

$$\beta = v\left(\left(\sum_{j \geq 1} h_j p^{j-1} - 1\right)!\right) - \sum_{j \geq 1} ((j-1)h_j + v(h_j!)).$$

For  $j \geq 3$  and  $h_j \neq 0$ ,

$$\begin{aligned} v((h_j p^{j-1} - 1)!) &= h_j p^{j-2} - 1 + v((h_j p^{j-2} - 1)!) \\ &\geq h_j p^{j-2} - 1 + v((h_j p - 1)!) \\ &\geq (j-1)h_j + v(h_j!) \end{aligned}$$

since  $p^{j-2} - j + 1 \geq 1$ . So if there exists a  $j \geq 3$  such that  $h_j \neq 0$ , then

$$\begin{aligned} v\left(\left(\sum_{j \geq 1} h_j p^{j-1} - 1\right)!\right) &\geq v(h_1!) + v((h_2 p)!) + \sum_{j \geq 3} v((h_j p^{j-1} - 1)!) \\ &\geq \sum ((j-1)h_j + v(h_j!)). \end{aligned}$$

That is,  $\beta \geq 0$ . Hence  $v(\tau_u) \geq m - 1 \geq s(p - 2) - 1$  by (3.1).

If for all  $j \geq 3$ ,  $h_j = 0$ , since  $m = s(p - 1)$ ,

$$n = h_1(p - 1) + h_2(p^2 - 1) = mp + i(p - 1) = s(p - 1)p + i(p - 1).$$

This implies that  $h_1 + h_2 + h_2 p = sp + i$ . Since  $d = h_1 + h_2 = i - kp$ ,

$$h_2 p = sp + (i - h_1 - h_2) = sp + kp.$$

Then  $h_2 = s + k \geq s$ . On the other hand,

$$\begin{aligned} v(\tau_u) &= v((h_1 p + h_2 p^2) - 2!) - (h_1 + 2h_2 + v(h_1!) + v(h_2!)) \\ &= h_1 + h_2 p - 1 + v((h_1 + h_2 p - 1)!) - (h_1 + 2h_2 + v(h_1!) + v(h_2!)) \\ &\geq h_2(p - 2) - 1 + v((h_2 p - 1)!) - v(h_2!) \\ &\geq s(p - 2) - 1 \end{aligned}$$

as desired.

Case 2. If there is exactly one part  $g \in \mathbf{Z}^+$  such that  $g \neq p^\alpha - 1$ ,  $u_g = 1$ , and if  $t \neq g$  and  $u_t \neq 0$  then  $t = p^\alpha - 1$ . In this case, we have  $d = \sum_{j \geq 1} h_j + 1$ ,

$$n = \sum_{j \geq 1} h_j (p^j - 1) + g = (m + i)p - i,$$

and

$$n + d - 2 = \sum_{j \geq 1} h_j p^j + g - 1 = (m + i)p - i + d - 2.$$

Then  $g = (m + i)p - i + d - 1 - \sum_{j \geq 1} h_j p^j$ .

Also we can check that

$$v(\gamma_u) = \sum_{j \geq 1} (jh_j + v(h_j!)) + v(g + 1). \quad (3.2)$$

Let  $\delta = i + 1 - d = i - \sum_{j \geq 1} h_j$ . Then  $\delta \geq 0$  since  $d \leq i + 1$ . We have

$$\delta + g = (i + 1 - d) + (m + i)p - i + d - 1 - \sum_{j \geq 1} h_j p^j = k'p,$$

where  $k' = m + i - \sum h_j p^{j-1}$ . Then

$$\sum_{j \geq 1} h_j p^{j-1} = m + i - k'.$$

Since  $g > 0$  and  $\delta \geq 0$ , we have  $k' > 0$ . Furthermore, if  $\delta = 0$ , then  $g = k'p$ .

On the other hand, since  $n = (m + i)p - i$ ,

$$n + d - 2 = (m + i)p - (\delta + 1) = (m + i - k')p + g - 1. \quad (3.3)$$

Hence by (2.2), (2.3), (3.2), (3.3) and Lemma 2.3,

$$\begin{aligned} v(\tau_u) &= v(((m + i - k')p + g - 1)!) - \left( \sum_{j \geq 1} (jh_j + v(h_j!)) + v(g + 1) \right) \\ &\geq v(((m + i - k')p)!) + v((g - 1)!) \\ &\quad - \sum_{j \geq 1} ((j - 1)h_j + v(h_j!)) - \sum_{j \geq 1} h_j - v(g + 1) \\ &\geq m + i - k' - \sum_{j \geq 1} h_j + v((m + i - k')!) + v((g - 1)!) \\ &\quad - v\left(\left(\sum_{j \geq 1} h_j p^{j-1}\right)!\right) - v(g + 1) \\ &\geq m + i - k' - \sum_{j \geq 1} h_j + v((g - 1)!) - v(g + 1) \\ &\geq m - 1 + \delta' \\ &\geq s(p - 2) - 1 + \delta', \end{aligned}$$

where

$$\delta' = \delta - k' + 1 + v((g - 1)!) - v(g + 1).$$

Thus it is sufficient to show that  $\delta' \geq 0$ .

If  $\delta - k' \geq 0$ , then by Lemma 2.4,

$$\delta' \geq v((g - 1)!) - v(g + 1) + 1 \geq 0.$$

It remains to consider the case  $\delta - k' < 0$ . In this case, let  $\delta = xp + r$  with  $0 \leq r < p$ . Then  $x = \lfloor \delta/p \rfloor$ . Clearly  $x < \delta$  unless  $\delta = 0 = r = x$ , and  $x < \delta - 1$  if  $\delta \geq 2$  since  $p \geq 3$ .

Since  $0 < g = k'p - \delta = (k' - x)p - r$ , we have  $k' - x \geq 1$ . But

$$g - 1 = (k' - x)p - (r + 1) = (k' - x - 1)p + (p - r - 1).$$

So

$$v((g - 1)!) = v(((k' - x - 1)p)!) = k' - x - 1 + v((k' - x - 1)!).$$

Hence

$$\begin{aligned} \delta' &= \delta - k' + 1 + k' - x - 1 + v((k' - x - 1)!) - v(g + 1) \\ &= \delta - x + v((k' - x - 1)!) - v(g + 1). \end{aligned}$$

If  $p \nmid g + 1$ , then  $\Delta' = \delta - x \geq 0$ . Now let  $p \mid g + 1$ . Since  $g + 1 = (k' - x)p - (r - 1)$ , we have  $r = 1$  and  $g + 1 = (k' - x)p$ . So

$$\delta' = \delta - x + v((k' - x - 1)!) - v(k' - x) - 1.$$

Since  $r \neq 0$ , we have  $\delta \neq 0$ . So  $\delta - x \geq 1$ . By Lemma 2.4 it remains to show that  $\delta - x = 1$  is impossible. If  $\delta - x = 1$ , then  $\delta = 1$  and  $x = 0$ , and it is sufficient to show that  $k' - x \neq p$ . But if  $k' = p$  then  $\delta + g = 1 + g = k'p = p^2$ , so  $g = p^2 - 1$ , which is impossible since  $g \neq p^\alpha - 1$ . The proof of Lemma 3.3 is complete.  $\square$

**COROLLARY 3.4.** *Let  $n = (m + i)p - i$  with  $m = s(p - 1)$ . Assume that  $w(u) = n$  and  $d(u) \leq i + 1$ . Then  $v(\tau_u) \geq s(p - 2) - 1$ .*

**PROOF.** This corollary follows immediately from Lemmas 3.2 and 3.3.  $\square$

Let us now recall the critical bounds for  $\hat{B}_n/n$ .

**LEMMA 3.5 [3].** *Let  $p$  be an odd prime. Suppose that  $w(u) = n$ ,  $n = (p - 1)s_0$  and  $u_{p-1} < s_0$ . Let  $e = v(\gamma_u) - v((pu_{p-1})!)$  and  $\hat{n} = n - (p - 1)u_{p-1}$ . Then*

$$n + d - 2 \geq (u_{p-1} + e + 1)p$$

except for the following cases where

$$(u_{p-1} + e + 1)p > n + d - 2 \geq (u_{p-1} + e)p :$$

- (i)  $p \geq 3$ ,  $u_{p-1} = s_0 - 1$ , and for  $1 \leq i \leq (p - 3)/2$ , we have  $u_i = u_{p-1-i}$ , or if  $i = (p - 1)/2$ , we have  $u_i = 2$ . In these cases,  $\hat{n} = p - 1$  and  $e = 0$ .
- (ii)  $p = 3$ ,  $u_2 = s_0 - 4$ ,  $u_8 = 1$ . In this case,  $\hat{n} = 8$  and  $e = 2$ .

For any positive integer  $x$ , by Lemma 2.2,

$$\frac{(xp)!}{x!p^x} - (-1)^x \equiv 0 \pmod{p^{v(x)+1}}.$$



Then associated to the prime number  $p$ , we can define an arithmetical function  $k_p$  for any positive integer  $x$  by

$$k_p(x) := \frac{1}{p^{v(x)+1}} \left( \frac{(xp)!}{x!p^x} - (-1)^x \right).$$

Clearly  $k_p(x) \in \mathbf{Z}$  for any positive integer  $x$  and  $k_p(1)$  is the usual *Wilson quotient* (see, for instance, [15]). We call  $k_p(x)$  the *generalized Wilson quotient*. On the other hand, for any positive integer  $x$ , we define

$$h_p(x) := \frac{(-1)^{x-1}(xp-2)!}{p^x x!}.$$

Then

$$h_p(x) = \frac{(-1)^{x-1}}{p^x} \prod_{i=1, p \nmid i}^{xp-2} i.$$

We have the following result.

**LEMMA 3.6.** *Let  $s$  and  $l$  be positive integers such that  $v_p(l) = N$ . If  $v(s) < N$ , then*

$$h_p(l+s) - h_p(s) \equiv g_p(l, s) \pmod{p^{N+1}},$$

where  $g_p(l, s)$  is defined by

$$g_p(l, s) := ((-1)^l s k_p(l) p^{N+1} - (-1)^s l k_p(s) p^{v(s)+1} - l) / (ps(l+s)) \pmod{p^{N+1}}.$$

**PROOF.** First since  $v(s) < N$ ,

$$\begin{aligned} \prod_{i=1, p \nmid i}^{(l+s)p-2} i &= \left( \prod_{i=1, p \nmid i}^{lp-1} i \right) \left( \prod_{i=lp+1, p \nmid i}^{(l+s)p-2} i \right) \\ &= \left( \prod_{i=1, p \nmid i}^{lp-1} i \right) \left( \prod_{i=1, p \nmid i}^{sp-2} (lp+i) \right) \\ &= \left( \prod_{i=1, p \nmid i}^{lp-1} i \right) \left( \prod_{i=1, p \nmid i}^{sp-2} i + lp \left( \prod_{i=1, p \nmid i}^{sp-2} i \right) \left( \sum_{j=1, p \nmid j}^{sp-2} j^{-1} \right) + (lp)^2 k_1 \right) \\ &= \left( \prod_{i=1, p \nmid i}^{lp-1} i \right) \left( \left( \prod_{i=1, p \nmid i}^{sp-2} i \right) \left( 1 + lp + (lp/2) \sum_{j=2, p \nmid j}^{sp-2} (j^{-1} + (sp-j)^{-1}) \right) + (lp)^2 k_1 \right) \\ &= \left( \prod_{i=1, p \nmid i}^{lp-1} i \right) \left( \left( \prod_{i=1, p \nmid i}^{sp-2} i \right) \left( 1 + lp + lp(sp/2) \sum_{j=2, p \nmid j}^{sp-2} (j(sp-j))^{-1} \right) + (lp)^2 k_1 \right) \\ &\equiv (1+lp) \left( \prod_{i=1, p \nmid i}^{lp-1} i \right) \left( \prod_{i=1, p \nmid i}^{sp-2} i \right) \pmod{p^{v(s)+N+2}}, \end{aligned} \tag{3.4}$$

where  $k_1$  is some positive integer.

Consequently, by the definition of  $k_p(s)$  we can easily show that

$$\prod_{i=1, p \nmid i}^{lp-1} i = \frac{(lp)!}{l!p^l} = (-1)^l + k_p(l)p^{N+1} \tag{3.5}$$

and

$$\prod_{i=1, p \nmid i}^{sp-2} i = (-1)(1-sp)^{-1}(sp)!/(s!p^s) = \left(-\sum_{j=0}^{\infty} (sp)^j\right)((-1)^s + k_p(s)p^{v(s)+1}). \tag{3.6}$$

Then by (3.4), (3.5) and (3.6) we can deduce that

$$\begin{aligned} &h_p(l+s) - h_p(s) \\ &= (-1)^{l+s-1}(p(l+s))^{-1} \prod_{i=1, p \nmid i}^{(l+s)p-2} i - (-1)^{s-1}(ps)^{-1} \prod_{i=1, p \nmid i}^{sp-2} i \\ &\equiv (-1)^{l+s-1}(p(l+s))^{-1}(1+lp) \left(\prod_{i=1, p \nmid i}^{lp-1} i\right) \left(\prod_{i=1, p \nmid i}^{sp-2} i\right) - (-1)^{s-1}(ps)^{-1} \prod_{i=1, p \nmid i}^{sp-2} i \\ &= (-1)^{s-1}(ps)^{-1} \left(\prod_{i=1, p \nmid i}^{sp-2} i\right) \left((-1)^l s(1+lp)(l+s)^{-1} \prod_{i=1, p \nmid i}^{lp-1} i - 1\right) \\ &= (-1)^{s-1}(ps)^{-1} \left(\prod_{i=1, p \nmid i}^{sp-2} i\right) \left((-1)^l s(1+lp)(l+s)^{-1}((-1)^l + k_p(l)p^{N+1}) - 1\right) \\ &\equiv (-1)^{s-1}(ps)^{-1} \left(\prod_{i=1, p \nmid i}^{sp-2} i\right) (s(l+s)^{-1}((-1)^l k_p(l)p^{N+1} + lp) - l(l+s)^{-1}) \\ &\equiv (-1)^{s-1} \left(\prod_{i=1, p \nmid i}^{sp-2} i\right) ((-1)^l k_p(l)p^N(l+s)^{-1} + l(l+s)^{-1} - l(ps(l+s))^{-1}) \\ &= (-1)^s \left(\sum_{j=0}^{\infty} (sp)^j\right) ((-1)^s + k_p(s)p^{v(s)+1}) (((-1)^l k_p(l)p^N + l)(l+s)^{-1} - l(ps(l+s))^{-1}) \\ &\equiv (1+sp)(1 + (-1)^s k_p(s)p^{v(s)+1}) (((-1)^l k_p(l)p^N + l)(l+s)^{-1} - l(ps(l+s))^{-1}) \\ &\equiv g_p(l, s) \pmod{p^{N+1}} \end{aligned}$$

as required. Thus Lemma 3.6 is proved. □

Using the generalized Wilson quotient, we can now establish the universal Kummer congruences modulo powers of odd primes. This is the first main result of this paper.

**THEOREM 3.7.** *Let  $n = m + l(p - 1)$  and  $p^N \mid l$ . Suppose that  $m = s(p - 1)$  and  $s \geq \lceil (N + 2)/(p - 2) \rceil$ .*

(i) If  $p \geq 5$ , then

$$\hat{B}_n/n \equiv c_{p-1}^l \hat{B}_m/m + g_p(l, s)c_{p-1}^{l+s} \pmod{p^{N+1}\mathbf{Z}_p[c_1, \dots, c_n]}.$$

(ii) If  $p = 3$ , then

$$\hat{B}_n/n \equiv c_2^l \hat{B}_m/m + g_3(l, s)c_2^{l+s} + \Psi c_2^{l+s-4}c_8 \pmod{3^{N+1}\mathbf{Z}_3[c_1, \dots, c_n]},$$

where  $\Psi = 0$  if  $s \equiv 1 \pmod{3}$ ,  $\Psi = -l$  if  $s \equiv 0 \pmod{3}$ , and  $\Psi = l$  if  $s \equiv -1 \pmod{3}$ .

**PROOF.** First consider the terms  $\tau_u c^u$  of  $\hat{B}_n/n$  where  $u_{p-1} \geq l$ . Let  $u'_{p-1} = u_{p-1} - l := q$  and  $u'_i = u_i$  for  $i \neq p - 1$ . Then  $w(u') = m$  and  $c^{u'} c^l_{p-1} = c^u$ . It follows from (2.1) that

$$\frac{\hat{B}_n}{n} - c^l_{p-1} \frac{\hat{B}_m}{m} = \sum_{w(u)=n, u_{p-1} \geq l} (\tau_u - \tau_{u'})c^u + \sum_{w(u)=n, u_{p-1} < l} \tau_u c^u.$$

If  $u_{p-1} = n/(p - 1) = l + s$ , then  $u'_{p-1} = s = m/(p - 1)$ . Hence by the definition and Lemma 3.6,

$$\tau_u - \tau_{u'} = h_p(l + s) - h_p(s) \equiv g_p(l, s) \pmod{p^{N+1}}.$$

Next assume that  $u_{p-1} < l + s$ . Now let  $\dot{u}_{p-1} = 0$  and  $\dot{u}_i = u_i$  for  $i \neq p - 1$ .

Let  $v(\gamma_{\dot{u}}) = e$ . Then  $\gamma_{\dot{u}} = \varepsilon p^e$  where  $p \nmid \varepsilon$ . Since  $d' = d(u') = d(u) - l$  and  $\dot{d} = d(\dot{u}) = d' - q$ ,

$$n + d - 2 = lp + m + d' - 2 = lp + qp + \dot{n} + \dot{d} - 2.$$

Also  $\gamma_u = (l + q)!p^{l+q}\gamma_{\dot{u}}$  and  $\gamma_{u'} = q!p^q\gamma_{\dot{u}}$ .

If  $e = 0$ , then  $(\gamma_{\dot{u}}, p) = 1$ . So applying Lemma 2.5(ii) with  $a = \dot{n} + \dot{d} - 2$  gives us

$$\tau_u \equiv \tau_{u'} \pmod{p^{N+1}}.$$

If  $e > 0$ , then by Lemma 3.5 we have  $\dot{n} + \dot{d} - 2 \geq (e + 1)p$  with the exception of case (ii) where  $\dot{n} = 8$ ,  $e = 2$ , and  $u_2 = l + s - 4$ ,  $u_8 = 1$ . Hence by Lemma 2.5(iv),  $\tau_u \equiv \tau_{u'} \pmod{p^{N+1}}$  without the exceptional case.

We now turn to the exceptional term, which occurs if and only if  $p = 3$ ,  $u_2 = l + s - 4$ ,  $u_8 = 1$ . In this case,  $d = l + s - 4 + 1 = l + s - 3$ ,  $d' = s - 3$ . Then

$$n + d - 2 = 2(l + s) + l + s - 3 - 2 = 3(l + s) - 5$$

and

$$n' + d' - 2 = m + d' - 2 = 3s - 5.$$

Also

$$\gamma_u = 3^{l+s-4} \cdot 9 \cdot (l + s - 4)! = 3^{l+s-2}(l + s - 4)!$$

and

$$\gamma_{u'} = 3^{s-4} \cdot 9 \cdot (s - 4)! = 3^{s-2}(s - 4)!.$$

Hence by Lemmas 2.2 and 2.5(ii),

$$\begin{aligned} \tau_u &= (-1)^{d-1}(3(l+s)-5)!3^{-(l+s-2)}((l+s-4)!)^{-1} \\ &= (-1)^{d-1}(3(l+s)-5)!3^{-(l+s-2)}((l+s-2)!)^{-1}(l+s-3)(l+s-2) \\ &= (-1)^{d-1}(3(l+s)-5)!3^{-(l+s-2)}((l+s-2)!)^{-1}(l^2+l(2s-5)+(s-2)(s-3)) \\ &\equiv (-1)^{d-1}(-1)^l(3s-5)!3^{2-s}((s-2)!)^{-1}l(2s-5) \\ &\quad + (-1)^{d-1}(-1)^l(3s-5)!3^{2-s}((s-2)!)^{-1}(s-2)(s-3) \\ &\equiv (-1)^{s-4}l(3s-5)!3^{2-s}((s-2)!)^{-1}(2s-5) + \tau_{u'} \pmod{3^{N+1}}. \end{aligned}$$

But by Lemma 2.1,

$$\begin{aligned} (3s-5)!3^{2-s}((s-2)!)^{-1}(2s-5) &= (3s-6)!3^{2-s}((s-2)!)^{-1}(3s-5)(2s-5) \\ &\equiv (-1)^{s-2}(-1)(2s-2) \pmod{3}. \end{aligned}$$

So

$$\tau_u \equiv (-1)^{s-4+s-2+1}(2s-2)l + \tau_{u'} \equiv (-1)l(2s-2) + \tau_{u'} \pmod{3^{N+1}}.$$

Thus  $\tau_u \equiv \tau'_u \pmod{3^{N+1}}$  if  $s \equiv 1 \pmod{3}$ ,  $\tau_u \equiv \tau'_u - l \pmod{3^{N+1}}$  if  $s \equiv 0 \pmod{3}$  and  $\tau_u \equiv \tau_{u'} + l \pmod{3^{N+1}}$  if  $s \equiv -1 \pmod{3}$ .

We can now deal with the terms where  $u_{p-1} < l$ . In what follows we assume that  $u_{p-1} = l - x$  with  $x \geq 1$ . To finish the proof, it is sufficient to show that if  $w(u) = n$  and  $u_{p-1} < l$  then  $\tau_u \equiv 0 \pmod{p^{N+1}}$  if  $s \geq \lceil (N+2)/(p-2) \rceil$ , with the single exception where  $p = 3$  and  $u$  is given by  $u_{p-1} = l + s - 4, u_8 = 1$ .

If  $n + d - 2 \geq lp$ , then there exists an integer  $k$  such that

$$(l+k)p \leq n+d-2 < (l+k+1)p.$$

With our usual notation,

$$\dot{n} = n - (l-x)(p-1) = m + x(p-1).$$

Let  $e = v(\gamma_{\dot{u}})$ . Since  $u_{p-1} = l - x < l$ ,

$$n + d - 2 \geq (l - x + e + 1)p \tag{3.7}$$

with the exceptional case (ii) of Lemma 3.5 which was previously considered.

On the other hand,

$$\begin{aligned} v(\tau_u) &= v((n+d-2)!) - (l-x) - v((l-x)!) - e \\ &\geq v(((l+k)p)!) - (l-x) - v((l-x)!) - e \\ &= (l+k) + v((l+k)!) - (l-x) - v((l-x)!) - e \\ &\geq k + x + v(l) - e. \end{aligned}$$

Suppose now that  $v(\tau_u) < v(lp)$ . Then  $e > k + x - 1$ , that is,  $e \geq k + x$ . But by (3.7),

$$n + d - 2 \geq (l - x + e + 1)p \geq (l - x + k + x + 1)p = (l + k + 1)p$$

which contradicts  $(l + k + 1)p > n + d - 2$ . Thus in this case we infer that  $v(\tau_u) \geq v(lp) \geq N + 1$ .

Now it remains to consider the case  $n + d - 2 < lp$ . In this case,

$$n + d = m + l(p - 1) + d < lp + 2,$$

that is,  $m + d \leq l + 1$ . Since  $u_{p-1} = l - x < d \leq l + 1 - m$ ,  $x \geq m$ . One may let  $x = m + i$  with  $i \geq 0$ . Then

$$w(\dot{u}) = n - u_{p-1}(p - 1) = m + x(p - 1) = (m + i)p - i$$

and

$$d(\dot{u}) = d - (l - x) \leq x + 1 - m = i + 1.$$

But  $u_{p-1} = l - x$ . So  $n + d - 2 \geq (l - x)p + \dot{n} + \dot{d} - 2$  and  $v(\tau_u) \geq v(\tau_{\dot{u}})$ . Since  $s \geq [(N + 2)/(p - 2)]$ , then by assumption and replacing  $n$  and  $u$  by  $\dot{n} = (m + i)p - i$  and  $\dot{u}$ , respectively, Corollary 3.4 gives  $\tau_u \equiv 0 \pmod{p^{N+1}}$ .

The proof of Theorem 3.7 is complete. □

### 4. Auxiliary results for powers of 2

In the current section, we deal with the even prime  $p = 2$  case. In order to establish the universal Kummer congruences modulo powers of 2, we provide a detailed 2-adic analysis for many kinds of factorials and double factorials. First we give several congruences modulo powers of 2 for double factorials.

**LEMMA 4.1** [3]. *Each of the following is true.*

- (i) *If  $k$  is odd, then  $(2k - 1)!! \equiv (-1)^{(k-1)/2} \pmod{4}$ .*
- (ii) *If  $k \geq 1$ , then  $(4k - 3)!! \equiv (-1)^{k-1} \pmod{16}$ .*
- (iii) *If  $k \geq 1$  and  $N \geq 3$ , then  $(k2^N - 3)!! \equiv -1 \pmod{2^{N+1}}$ .*

**LEMMA 4.2.** *Let  $k \geq 1$ ,  $N \geq 3$  and  $a \geq 2$  be integers. Then:*

- (i)  $(k2^N + 2a - 3)!! / (k2^N + 1)!! \equiv \begin{cases} (2a - 3)!! \pmod{2^{N+1+\min\{v(a), N-1\}}} & \text{if } 2 \mid a, \\ (2a - 3)!! + k2^N \pmod{2^{N+1}} & \text{if } 2 \nmid a; \end{cases}$
- (ii)  $(k2^N + 2a - 3)!! \equiv \begin{cases} (2a - 3)!! \pmod{2^{N+1}} & \text{if } 2 \mid a, \\ (2a - 3)!! + k2^N \pmod{2^{N+1}} & \text{if } 2 \nmid a; \end{cases}$
- (iii) *If  $k$  is odd,*

$$(k2^N - 3)!! \equiv \begin{cases} -1 + (-1)^{(k-1)/2} 2^{N+1} \pmod{2^{N+3}} & \text{if } N = 3, \\ -1 + (-1)^{(k+1)/2} 2^{N+1} \pmod{2^{N+3}} & \text{if } N \geq 4. \end{cases}$$

*In particular, we have  $(k2^N - 3)!! \equiv -1 + 2^{N+1} \pmod{2^{N+2}}$ .*

**PROOF.** (i) First

$$\begin{aligned}
 (k2^N + 2a - 3)!! / (k2^N + 1)!! &= (k2^N + 3)(k2^N + 5) \cdots (k2^N + 2a - 3) \\
 &= (2a - 3)!! + k2^N \sum_{j \in S} (2a - 3)!! / j + x(k2^N)^2 \\
 &\equiv (2a - 3)!! + k2^N \sum_{j \in S} (2a - 3)!! / j \pmod{2^{2N}},
 \end{aligned}
 \tag{4.1}$$

where  $x \in \mathbb{N}$  and  $S = \{3, 5, \dots, 2a - 3\}$ . If  $j \in S$ , then  $2a - j \in S$ . Clearly  $j \neq 2a - j$  unless  $j = a \in S$ . If  $2 \mid a$ , then  $a \notin S$ . Therefore

$$\begin{aligned}
 \sum_{j \in S} \frac{(2a - 3)!!}{j} &= \sum_{j \in S, j < a} \left( \frac{(2a - 3)!!}{2a - j} + \frac{(2a - 3)!!}{j} \right) \\
 &= 2a \sum_{j \in S, j < a} \frac{(2a - 3)!!}{j(2a - j)}.
 \end{aligned}$$

Then

$$v\left(k2^N \sum_{j \in S} \frac{(2a - 3)!!}{j}\right) \geq N + 1 + v(a).$$

Hence by (4.1), Lemma 4.2(i) is true for the case  $2 \mid a$ .

Now we consider the case  $2 \nmid a$ , then  $a \in S$ . Hence

$$\begin{aligned}
 \sum_{j \in S} \frac{(2a - 3)!!}{j} &= \sum_{j \in S, j < a} \left( \frac{(2a - 3)!!}{2a - j} + \frac{(2a - 3)!!}{j} \right) + \frac{(2a - 3)!!}{a} \\
 &= 2a \sum_{j \in S, j < a} \frac{(2a - 3)!!}{j(2a - j)} + \frac{(2a - 3)!!}{a}.
 \end{aligned}$$

Then  $v(\sum_{j \in S} (2a - 3)!! / j) = 0$  since  $v((2a - 3)!! / a) = 0$ . Thus by (4.1) we infer that Lemma 4.2(i) holds for the case  $2 \nmid a$ . Part (i) is proved.

(ii) Since  $N \geq 3$ ,  $2N \geq N + 1$ . Then by Lemma 4.1(iii),

$$\begin{aligned}
 (k2^N + 1)!! &= (k2^N - 3)!!(k2^N - 1)(k2^N + 1) \\
 &\equiv -(k2^N - 3)!! \\
 &\equiv 1 \pmod{2^{N+1}}.
 \end{aligned}$$

So the desired result follows immediately from part (i).

(iii) If  $k \equiv 1 \pmod{4}$ , then by part (ii),

$$(k2^N - 3)!! = (t_1 2^{N+2} + 2^N - 3)!! \equiv (2^N - 3)!! \pmod{2^{N+3}},
 \tag{4.2}$$

where  $t_1 \geq 0$  is an integer. If  $k \equiv 3 \pmod{4}$ , then by part (ii),

$$(k2^N - 3)!! = (t_2 2^{N+2} + 3 \cdot 2^N - 3)!! \equiv (3 \cdot 2^N - 3)!! \pmod{2^{N+3}},
 \tag{4.3}$$

where  $t_2 \geq 0$  is an integer. By part (i),

$$\begin{aligned} (3 \cdot 2^N - 3)!! &\equiv (2^{N+1} + 2^N - 3)!!((2^{N+1} + 1)!!)^{-1}(-1) \\ &\quad \times (2^N + 2^N - 3)!!((2^N + 1)!!)^{-1}(-1)(2^N - 3)!! \\ &\equiv ((2^N - 3)!!)^3 \pmod{2^{2N}}. \end{aligned} \tag{4.4}$$

Since  $N \geq 3$ ,  $2N \geq N + 3$ . Then by (4.3) and (4.4),

$$(k2^N - 3)!! \equiv ((2^N - 3)!!)^3 \pmod{2^{N+3}}. \tag{4.5}$$

First consider the case  $N = 3$ . Clearly  $(2^3 - 3)!! \equiv 15 \pmod{2^6}$ . Hence by (4.2),

$$(k2^3 - 3)!! \equiv 15 = -1 + (-1)^{(k-1)/2}2^4 \pmod{2^6}$$

if  $k \equiv 1 \pmod{4}$ . By (4.5),

$$(k \cdot 2^3 - 3)!! \equiv 15^3 \equiv -17 = -1 + (-1)^{(k-1)/2}2^4 \pmod{2^6}$$

if  $k \equiv 3 \pmod{4}$ . Part (iii) is proved for the  $N = 3$  case. In what follows we deal with the  $N \geq 4$  case.

We claim that  $(2^N - 3)!! \equiv -1 - 2^{N+1} \pmod{2^{N+3}}$  for  $N \geq 4$ . We use induction on  $N$ . Evidently  $(2^4 - 3)!! \equiv -1 - 2^5 \pmod{2^7}$  if  $N = 4$ . Assume that  $(2^N - 3)!! \equiv -1 - 2^{N+1} \pmod{2^{N+3}}$  for some  $N \geq 4$ . Since  $N \geq 4$ ,  $2N \geq N + 4$ . Then by part (i) and the induction hypothesis,

$$\begin{aligned} (2^{N+1} - 3)!! &\equiv (2^N + 2^N - 3)!!((2^N + 1)!!)^{-1}(-1)(2^N - 3)!! \\ &\equiv -((2^N - 3)!!)^2 \\ &\equiv -1 - 2^{N+2} \pmod{2^{N+4}}. \end{aligned}$$

Hence the claim is true. So the desired result follows immediately from the claim and (4.2), (4.5). Part (iii) is proved. □

**LEMMA 4.3.** *Let  $a \geq 0$  and  $i \geq 1$  be integers. Define*

$$f_a(i, j) := (a + 1) \cdots (a + 2i)/(a + j)$$

for  $j \in \{1, \dots, 2i\}$ . Then

$$v\left(\sum_{j=1}^{2i} f_a(i, j)\right) \geq \begin{cases} i - 1 & \text{if } 1 \leq i \leq 3, \\ i & \text{otherwise.} \end{cases}$$

**PROOF.** First

$$v(f_a(1, 1) + f_a(1, 2)) = v(2a + 3) = 0.$$

So Lemma 4.3 is true for  $i = 1$ . For  $i = 2$ , we can easily check that

$$\sum_{j=1}^4 f_a(2, j) \equiv 2a(a + 1) + 2 \equiv 2 \pmod{4}.$$

Hence  $v(\sum_{j=1}^4 f_a(2, j)) = 1$  as required. Lemma 4.3 is true when  $i = 2$ . For  $i = 3$ , by the fact that 8 divides the product of any four consecutive integers, we get  $8 \mid f_a(3, j)$  for  $j = 1, 2, 5, 6$ . On the other hand,

$$f_a(3, 3) \equiv a^3(a + 1)^2 \equiv 0 \pmod{4}$$

and

$$f_a(3, 4) \equiv a^2(a + 1)^2(a + 3) \equiv 0 \pmod{4}.$$

It follows that

$$v\left(\sum_{j=1}^6 f_a(3, j)\right) \geq \min_{1 \leq j \leq 6} \{v(f_a(3, j))\} \geq 2$$

as required.

Now let  $i \geq 4$ . We may let  $a = 2b + b'$ , where  $b \in \mathbf{Z}_{\geq 0}$  and  $b' = 0$  or  $1$ . Then

$$\begin{aligned} v(f_a(i, j)) &= v((2b + 2) \cdots (2b + 2i)/(2b + j + b')) \\ &= i + v((b + 1) \cdots (b + i)/(2b + j + b')). \end{aligned} \tag{4.6}$$

If  $2 \nmid (b' + j)$ , then

$$v((b + 1) \cdots (b + i)/(2b + j + b')) \geq 3.$$

If  $2 \mid (b' + j)$ , then

$$b + (j + b')/2 \in \{b + 1, \dots, b + i\}.$$

Thus

$$v((b + 1) \cdots (b + i)(2b + (j + b')/2))^{-1} \geq 0$$

since  $i \geq 4$ . Hence by (4.6), we have  $v(f_a(i, j)) \geq i$  for all  $1 \leq j \leq 2i$ . Therefore

$$v\left(\sum_{j=1}^{2i} f_a(i, j)\right) \geq \min_{1 \leq j \leq 2i} \{v(f_a(i, j))\} \geq i.$$

The proof of Lemma 4.3 is complete. □

**REMARK 4.4.** In fact, we infer that

$$v((b + 1) \cdots (b + i)(2b + j + b')^{-1}) \geq 1$$

for  $i \geq 6$  and

$$v((b + 1) \cdots (b + i)(2b + j + b')^{-1}) \geq 3$$

for  $i \geq 8$ . Then  $v(f_a(i, j)) \geq i + 1$  for  $i \geq 6$  and  $v(f_a(i, j)) \geq i + 3$  for  $i \geq 8$  by (4.6).



**LEMMA 4.5.** *Let  $q, r, a \in \mathbf{N}$ ,  $e \in \mathbf{Z}^+$  and  $v(l) = N$ . Define  $\delta_r = l$  for  $r = 1, 2$  and  $\delta_r = 0$  for  $r \neq 1, 2$ . Each of the the following is true.*

- (i)  $(l + q + 2r)! / ((l + q)!r!) \equiv (q + 2r)! / (q!r!) + \delta_r \pmod{2^{N+1}}$ .
- (ii) *If  $a = 0$  or  $1$ , then*

$$\begin{aligned} & (2(l + q + 2r) + a)! / (2^{l+q+2r}(l + q)!r!) \\ & \equiv (2(q + 2r) + a)! / (2^{q+2r}q!r!) + \delta_r \pmod{2^{N+1}}. \end{aligned}$$

- (iii) *If  $a \geq 2e$ , then*

$$(2(l + q + 2r) + a)! / (2^{l+q+2r}(l + q)!r!) \equiv (2(q + 2r) + a)! / (2^{q+2r}q!r!) \pmod{2^{N+e}}$$

- (iv) *If  $a \geq 2(e + 1)$ , then*

$$\begin{aligned} & (2(l + q + 2r) + a)! / (2^{l+q+2r+e}(l + q)!r!) \\ & \equiv (2(q + 2r) + a)! / (2^{q+2r+e}q!r!) \pmod{2^{N+1}}. \end{aligned}$$

**PROOF.** (i) For  $r = 0$ , the congruence is trivial. Now let  $r > 0$ . If  $r \geq N + 1$ ,

$$v((l + q + 2r)! / ((l + q)!r!)) \geq v((2r)!) - v(r!) = r \geq N + 1$$

since

$$v((l + q + 2r)!) \geq v((l + q)!) + v((2r)!)$$

and  $v((2r)!) = r + v(r!)$ . Similarly, we have  $v((q + 2r)! / (q!r!)) \geq N + 1$ . Then

$$(l + q + 2r)! / ((l + q)!r!) \equiv (q + 2r)! / (q!r!) \equiv 0 \pmod{2^{N+1}}$$

as required. If  $r \leq N$ , then  $v(r!) \leq r - 1 \leq N - 1$ . On the other hand,

$$\begin{aligned} (l + q + 2r)! / ((l + q)!r!) &= (l + q + 1) \cdots (l + q + 2r) / r! \\ &\equiv (q + 1) \cdots (q + 2r) / r! + (l/r!) \sum_{j=1}^{2r} (q + 1) \cdots (q + 2r) / (q + j) \\ &\equiv (q + 2r)! / (q!r!) + (l/r!) \sum_{j=1}^{2r} f_q(r, j) \pmod{2^{N+1}}, \end{aligned} \tag{4.7}$$

where  $f_a(i, j)$  is defined as in Lemma 4.3. From (4.7) and Lemma 4.3 we deduce that if  $r = 1, 2$ , then

$$(l + q + 2r)! / ((l + q)!r!) \equiv (q + 2r)! / (q!r!) + l \pmod{2^{N+1}},$$

and if  $r \geq 3$ , then

$$(l + q + 2r)! / ((l + q)!r!) \equiv (q + 2r)! / (q!r!) \pmod{2^{N+1}}.$$

So part (i) is proved.

(ii) Since  $v(2l) = N + 1$ ,

$$(2l + 2q + 4r \pm 1)!! \equiv (2q + 4r \pm 1)!! \pmod{2^{N+1}} \tag{4.8}$$

by Lemma 4.2(ii). Then multiplying congruence (i) by (4.8) and noting that  $(2q + 4r \pm 1)!! \equiv 1 \pmod{2}$ , the desired result follows.

(iii) To deduce part (iii), let  $S = \{2, 4, \dots, 2e\}$ . Then

$$\begin{aligned} \prod_{x=1}^a (2(l + q + 2r) + x) &= \left( \prod_{i=1}^e 2(l + q + 2r + i) \right) \left( \prod_{x \notin S, x=1}^a (2(l + q + 2r) + x) \right) \\ &= 2^e \left( \prod_{i=1}^e (l + q + 2r + i) \right) \left( \prod_{x \notin S, x=1}^a (2l + 2q + 4r + x) \right). \end{aligned}$$

Thus, using congruence (ii)  $\pmod{2^N}$  for  $a = 0$ ,

$$\begin{aligned} &(2(l + q + 2r) + a)! / (2^{l+q+2r} l! q! r!) \\ &\equiv \left( \prod_{x=1}^a (2(l + q + 2r) + x) \right) (2(l + q + 2r))! / (2^{l+q+2r} l! q! r!) \\ &\equiv 2^e \left( \prod_{i=1}^e (q + 2r + i) \right) \left( \prod_{x \notin S, x=1}^a (2q + 4r + x) \right) (2(q + 2r))! / (2^{q+2r} q! r!) \\ &\equiv (2(2 + 2r) + a)! / (2^{q+2r} q! r!) \pmod{2^{N+e}}. \end{aligned}$$

(iv) To deduce part (iv), use the congruence (iii) with  $e$  replaced by  $e + 1$  and then divide by  $2^e$ . Thus Lemma 4.5 is proved. □

**LEMMA 4.6.** Let  $n = l + m$ ,  $N \geq 3$  and  $l = k2^N$ ,  $k \in \mathbf{Z}^+$ ,  $2 \nmid k$ . Let

$$g(a) := (-1)^{a-1} (2a - 3)!! / (2a)$$

for any integer  $a > 1$ . Then

$$g(n) \equiv g(m) + \begin{cases} (-1)^{(m-1)/2} l/2 & \pmod{2^{N+1}} & \text{if } 2 \nmid m, \\ l + l/(2mn) & \pmod{2^{N+1}} & \text{if } 2 \mid m, 4 \nmid m, \\ l - l/(2mn) & \pmod{2^{N+1}} & \text{if } 4 \mid m, 8 \nmid m. \end{cases}$$

**PROOF.** If  $2 \nmid m$ , then applying Lemma 4.2(ii),

$$(2n - 3)!! = (2l + 2m - 3)!! \equiv (2m - 3)!! + 2l \pmod{2^{N+2}}.$$

By Lemma 4.1(i),

$$(2m - 3)!! = (2m - 3)(2(m - 2) - 1)!! \equiv (-1)^{(m-1)/2} \pmod{4}.$$

Since  $2 \nmid m$  and  $n = l + m$ ,

$$1/(mn) = 1/(m^2 + ml) \in 1 + 4\mathbf{Z}_2.$$

Thus

$$\begin{aligned} g(n) - g(m) &\equiv (2m - 3)!!(-l/(2mn)) + l/n \\ &\equiv (-1)^{(m-1)/2}(-l/2) + l \\ &\equiv (-1)^{(m-1)/2}l/2 \pmod{2^{N+1}}. \end{aligned}$$

If  $2 \mid m$ , then by Lemma 4.2(i),

$$(2n - 3)!! = (2l + 2m - 3)!! \equiv -(2l - 3)!!(2m - 3)!! \pmod{2^{N+2+\min\{v(m),N\}}}.$$

Thus for  $v(m) < N$ ,

$$g(n) - g(m) \equiv ((2l - 3)!!2^{-1}(l + m)^{-1} + (2m)^{-1})(2m - 3)!! \pmod{2^{N+1}}. \tag{4.9}$$

If  $2 \mid m$  and  $4 \nmid m$ , then  $(2m - 3)!! \equiv 1 \pmod{16}$  by Lemma 4.1(ii). Thus applying (4.9) and Lemma 4.2(iii) gives us

$$\begin{aligned} g(n) - g(m) &\equiv ((-1 + 2^{N+2})2^{-1}(l + m)^{-1} + (2m)^{-1})(2m - 3)!! \\ &\equiv 2^N(l/2 + m/2)^{-1} + l(2m(m + l))^{-1} \pmod{2^{N+1}}. \end{aligned} \tag{4.10}$$

Since  $l/2 + m/2 \in 1 + 2\mathbf{Z}_2$ , we have by (4.10) that

$$g(n) - g(m) \equiv l + l/(2mn) \pmod{2^{N+1}}.$$

If  $4 \mid m$  and  $8 \nmid m$ , then we may assume that  $m = 4\lambda$  with  $2 \nmid \lambda$ . Hence by Lemma 4.2(iii),

$$(2m - 3)!! \equiv -1 + (-1)^{(\lambda-1)/2}2^4 \equiv -1 + 4m \pmod{2^6}. \tag{4.11}$$

Also by Lemma 4.2(iii) and noting that  $N \geq 3$ ,

$$(2l - 3)!! = (k \cdot 2^{N+1} - 3)!! \equiv -1 + (-1)^{(k+1)/2}2^{N+2} \pmod{2^{N+4}}. \tag{4.12}$$

Thus using (4.9), (4.11) and (4.12),

$$\begin{aligned} g(n) - g(m) &\equiv ((-1 + (-1)^{(k+1)/2}2^{N+2})(2(l + m))^{-1} + (2m)^{-1})(2m - 3)!! \\ &\equiv ((-1)^{(k+1)/2}2^{N+1}(l + m)^{-1} + l(2m(l + m))^{-1})(-1 + 4m) \\ &\equiv ((-1)^{(k-1)/2}2^{N+1} + 2l)(l + m)^{-1} - l(2mn)^{-1} \\ &\equiv l - l(2mn)^{-1} \pmod{2^{N+1}}. \end{aligned}$$

The proof of Lemma 4.6 is complete. □

In the rest of this paper, we always let

$$e := v(\gamma_u) - v((2u_1)!) - (2u_3 + v(u_3!))$$

and define  $\dot{u}$  by:  $\dot{u}_1 = \dot{u}_3 = 0$  and  $\dot{u}_i = u_i$  for  $i \neq 1, 3$ . Let  $\dot{n} = w(\dot{u})$ . Then  $\dot{n} = n - u_1 - 3u_3$  and  $v(\gamma_{\dot{u}}) = e$ .

**LEMMA 4.7.** *Suppose that  $w(u) = n$ . Then  $n + d - 2 = 2(u_1 + 2u_3 + e) + \Gamma$ , where:*

- (i)  $\Gamma = -2$  if  $\dot{n} = 0$ ;
- (ii)  $\Gamma = 0$  if  $\dot{n} = 7 \cdot 2^\alpha$  and  $u_7 = 2^\alpha$ ,  $\alpha \in \mathbf{N}$ ;
- (iii)  $\Gamma = 1$  if  $\dot{n} = 2$ ;
- (iv)  $\Gamma \geq 2$  otherwise.

**PROOF.** If  $\dot{n} = 0$  that is,  $n = u_1 + 3u_3$ , we have  $e = 0$  and  $n + d - 2 = 2u_1 + 4u_3 - 2$ . Then  $\Gamma = -2$ .

Now we assume that  $\dot{n} > 0$ . Let  $\dot{u}_1 = \dot{u}_3 = 0$  and  $\dot{u}_i = u_i$  ( $i \neq 1, 3$ ). Then  $w(\dot{u}) = \dot{n}$ ,  $v(\gamma_{\dot{u}}) = e$  and

$$n + d - 2 = 2u_1 + 4u_3 + \dot{n} + d - 2.$$

So replacing  $u$  by  $\dot{u}$ , in what follows we can assume that  $u_1 = u_3 = 0$ . Note that  $n + d = \sum_{i=1}^n (i + 1)u_i$  and  $e = \sum_{i=1}^n e_i$ , where

$$e_i := v(i + 1)u_i + v(u_i!).$$

It follows immediately that  $e_i > 0$  if and only if either  $2 \mid (i + 1)$  or  $u_i \geq 2$ .

First consider case (ii):  $\dot{n} = 7 \cdot 2^\alpha$  and  $u_7 = 2^\alpha$ . Then

$$e_i = 3 \cdot 2^\alpha + v(2^\alpha!) = 4 \cdot 2^\alpha - 1.$$

Hence

$$(i + 1)u_i = 8u_7 = 2(e_7 + 1).$$

Since  $n + d - 2 = 8u_7 - 2$  and  $2(u_1 + 2u_3 + e) = 2e_7$ , we have  $\Gamma = 0$ .

For case (iii):  $\dot{n} = 2$ ,  $i = 2$ ,  $u_2 = 1$ . Clearly  $e_i = 0$ . Since  $u_1 = u_3 = e = 0$ ,

$$n + d - 2 = (i + 1)u_i - 2 = 1 = 2(u_1 + 2u_3 + e) + 1.$$

Hence  $\Gamma = 1$ .

In what follows we deal with case (iv). We claim that

$$(i + 1)u_i \geq 2(e_i + 1) + 2 = 2(v(i + 1)u_i + v(u_i!) + 1) + 2 \tag{4.13}$$

for all cases where  $i \neq 1, 3$  apart from cases (ii) and (iii).

If  $2 \nmid (i + 1)$  and  $u_i \geq 2$ , then  $e_i = v(u_i!) \leq u_i - 1$ . We can deduce that

$$(i + 1)u_i - 2 \geq 3u_i - 2 \geq 2u_i \geq 2(e_i + 1).$$

If  $2 \mid (i + 1)$ , we may let  $i + 1 = \varepsilon 2^t$  for some  $t \in \mathbf{N}$  with  $2 \nmid \varepsilon$ . Then  $e_i = tu_i + v(u_i!)$ ,  $(i + 1)u_i - 2 = \varepsilon 2^t u_i - 2$  and

$$2(e_i + 1) = 2(tu_i + v(u_i!)) + 1 \leq 2(t + 1)u_i.$$

For  $t \geq 4$ , we have  $2^t > 2(t + 2)$ . This implies that

$$(i + 1)u_i - 2 \geq 2^t u_i - 2 \geq 2(t + 1)u_i \geq 2(e_i + 1).$$

For  $t = 3$ , we have  $i + 1 = 2^3 \varepsilon$ . If  $\varepsilon \geq 3$ , then

$$(i + 1)u_i - 2 \geq 3 \cdot 2^3 u_i - 2 \geq 2(3 + 1)u_i \geq 2(e_i + 1).$$

If  $\varepsilon = 1$ , then

$$(i + 1)u_i - 2 = 2^3 u_i - 2 = 8u_i - 2$$

and

$$e_i = 3u_i + v(u_i!) = 3u_i + u_i - s(u_i).$$

Therefore

$$(i + 1)u_i - 2 \geq 2(e_i + 1)$$

if  $s(u_i) \geq 2$ . But if  $s(u_i) = 1$ , we have  $i = 7, u_i = 2^\alpha$ , which is case (ii).

For  $t = 1, 2$ , we have  $i + 1 = 2\varepsilon$  or  $2^2\varepsilon$ . Since  $i \neq 1, 3$ , we have  $\varepsilon \geq 3$ . Then

$$(i + 1)u_i - 2 \geq 3 \cdot 2^t u_i - 2 \geq 2(t + 1)u_i.$$

Hence the claim (4.13) holds as specified.

Finally, if  $u_i \geq 1$ , then  $(i + 1)u_i \geq 2$ , while if  $(i + 1)u_i \geq 2(e_i + 1)$  and  $(j + 1)u_j \geq 2(e_j + 1)$ , then

$$(i + 1)u_i + (j + 1)u_j - 2 \geq 2(e_i + e_j + 1).$$

So we have  $n + d - 2 \geq 2(e + 1)$  for case (iv), which follows by adding the ‘local’ inequalities for each value of  $i$  separately. □

**LEMMA 4.8.** *Let  $w(u) = n$ . Assume that  $\dot{n} > 0$ . Then  $v(\tau_u) \geq u_3 + \lceil \dot{n}/2 \rceil - 1$  except for  $\dot{n} = 7u_7$  where  $v(\tau_u) \geq u_3 + \lceil \dot{n}/2 \rceil - 3$ .*

**PROOF.** Let  $\dot{u}_1 = \dot{u}_3 = 0$  and  $\dot{u}_i = u_i (i \neq 1, 3)$ . Then  $w(\dot{u}) = \dot{n}$  and

$$n + d - 2 = 2u_1 + 4u_3 + \dot{n} + \dot{d} - 2.$$

So

$$\begin{aligned} v(\tau_u) &= v((n + d - 2)!) - v(\gamma_u) \\ &= v((2u_1 + 4u_3 + \dot{n} + \dot{d} - 2)!) - (u_1 + v(u_1!) + 2u_3 + v(u_3!)) - v(\gamma_{\dot{u}}) \\ &\geq v((4u_3)!) + v((\dot{n} + \dot{d} - 2)!) - 2u_3 - v(u_3!) - v(\gamma_{\dot{u}}) \\ &= u_3 + v((\dot{n} + \dot{d} - 2)!) - v(\gamma_{\dot{u}}). \end{aligned}$$

Noticing that  $v(\gamma_{\bar{u}}) = e = \sum e_i$ , it suffices to prove that

$$v((\dot{n} + \dot{d} - 2)!) - \sum_{i=1}^n e_i \geq \lceil \dot{n}/2 \rceil - 1.$$

We claim that

$$v(((i + 1)u_i - 2)!) - e_i \geq \lceil iu_i/2 \rceil - 1 \tag{4.14}$$

for  $u_i \geq 1$  and  $i \neq 1, 3, 7$ .

If  $2 \nmid (i + 1)$ , then

$$e_i = v(i + 1)u_i + v(u_i!) = v(u_i!)$$

and  $\lceil iu_i/2 \rceil = iu_i/2$ . Thus

$$v((i + 1)u_i - 2) \geq v(u_i!) + v((iu_i - 2)!) \geq v(u_i!) + iu_i/2 - 1 \geq e_i + \lceil iu_i/2 \rceil - 1$$

as claimed.

If  $2 \mid (i + 1)$ , we may let  $i + 1 = \delta 2^t$  where  $t \in \mathbf{Z}^+$  and  $2 \nmid \delta$ . Then  $e_i = tu_i + v(u_i!)$  and

$$(i + 1)u_i/2 = \delta 2^{t-1}u_i \geq \lceil iu_i/2 \rceil.$$

Therefore we obtain

$$\begin{aligned} v(((i + 1)u_i - 2)!) &= v((2(\delta 2^{t-1}u_i - 1)!)!) & (4.15) \\ &= \delta 2^{t-1}u_i - 1 + v((\delta 2^{t-1}u_i - 1)!) \\ &\geq \lceil iu_i/2 \rceil - 1 + v((\delta 2^{t-1}u_i - 1)!). \end{aligned}$$

Let  $\delta \geq 3$ . Then

$$v((\delta 2^{t-1}u_i - 1)!) \geq v((3 \cdot 2^{t-1}u_i - 1)!) \geq v((2tu_i)!) \geq tu_i + v((tu_i)!) \geq e_i$$

since  $3 \cdot 2^{t-1}u_i - 1 \geq 2tu_i$  for  $t \geq 1$  and  $u_i \geq 1$ . So the claim holds for this case by (4.15).

Now let  $\delta = 1$ , that is,  $i + 1 = 2^t$ . Since  $i \neq 1, 3, 7$ ,  $t \geq 4$ . Then by Lemma 2.1,

$$v((2^{t-1}u_i - 1)!) = 3 \cdot 2^{t-3}u_i - 2 + v((2^{t-3}u_i - 1)!) \geq tu_i + v(u_i!) \geq e_i$$

since  $3 \cdot 2^{t-3}u_i - 2 \geq tu_i$  and  $2^{t-3}u_i - 1 \geq u_i$  for  $t \geq 4$  and  $u_i \geq 1$ . So the claim holds for this case by (4.15).

On the other hand, if  $i \neq 1, 3, 7$ ,

$$v(((i + 1)u_i)!) \geq v(((i + 1)u_i - 2)!) + 1 \geq e_i + \lceil iu_i/2 \rceil$$

by claim (4.14). If  $i = 7$ , by Lemma 2.1,

$$v(8u_i!) = 7u_i + v(u_i!) \geq e_7 + \lceil 7u_7/2 \rceil.$$

Then for  $i \neq 1, 3$ ,

$$v((i + 1)u_i!) \geq e_i + \lceil iu_i/2 \rceil. \tag{4.16}$$

Moreover, if  $u_j \geq 1$  for some  $j \neq 7$ , then by (4.14) and (4.16),

$$\begin{aligned} v((\dot{n} + \dot{d} - 2)!) &= v\left(\left(\sum_{i=1}^n (i + 1)u_i - 2\right)!\right) \\ &= v\left(\left(\sum_{i=1, i \neq j}^n (i + 1)u_i + (j + 1)u_j - 2\right)!\right) \\ &\geq \sum_{i=1}^n e_i + \left\lceil 2^{-1} \sum_{i=1}^n iu_i \right\rceil - 1 \end{aligned}$$

as required. Finally, if  $\dot{n} = 7u_7$ , we can compute

$$v(\tau_u) \geq u_3 + v((8u_7 - 2)!) - e_7 \geq u_3 + 4u_7 - 3 - v(u_7).$$

We can easily show that

$$4u_7 - v(u_7) \geq \lceil 7u_7/2 \rceil = \lceil \dot{n}/2 \rceil.$$

Then  $v(\tau_u) \geq u_3 + \lceil \dot{n}/2 \rceil - 3$ . Lemma 4.8 is proved. □

### 5. Universal Kummer congruences for powers of 2

We are now in a position to give the universal Kummer congruences modulo powers of 2 in the form of Theorems 5.1 and 5.2. This is the second main result of this paper. We begin with Theorem 5.1.

**THEOREM 5.1.** *Let  $n \geq 2$  be an even number.*

(i) *If  $v(n) = 1$ , then*

$$\begin{aligned} \hat{B}_n/n &\equiv -c_1^n/(2n) + (n/2 - 1)c_1^{n-3}c_3 + 3(n - 4)c_1^{n-6}c_3^2/4 \\ &\quad - c_1^{n-2}c_2 + 2c_1^{n-5}(c_2c_3 + c_1c_4) \pmod{4\mathbf{Z}_2[c_1, \dots, c_n]}. \end{aligned}$$

(ii) *If  $v(n) \geq 2$ , then*

$$\begin{aligned} \hat{B}_n/n &\equiv ((2n)^{-1} - 2)c_1^n - 3(n - 2)c_1^{n-3}c_3/2 + (n - 4)c_1^{n-6}c_3^2/4 + (n - 8)c_1^{n-12}c_3^4/4 \\ &\quad - 3c_1^{n-2}c_2 + 2c_1^{n-4}c_4 + 4c_1^{n-4}c_2^2 + (n - 4)c_1^{n-8}c_2c_3(c_3 + c_1^3) \\ &\quad \pmod{8\mathbf{Z}_2[c_1, \dots, c_n]}. \end{aligned}$$

**PROOF.** By Lemma 4.8, and noting that  $\dot{n} = \sum_{i \neq 1,3} iu_i$ , we have only to consider the following cases.

(1)  $\dot{n} = 7, u_7 = 1, u_3 \leq 1$ . Then  $u_1 = n - 7 - 3u_3$ .

(2)  $\dot{n} = 6, u_1 = n - 6$ . In this case, we have  $u_2 = 3$ , or  $u_2 = u_4 = 1$ , or  $u_6 = 1$ .

(3)  $\dot{n} = 5, u_5 = 1$  and  $u_1 = n - 5$ .

(4)  $\dot{n} = 4, u_1 = n - 4 - 3u_3$  and  $u_3 \leq 1$ . In this case, either  $u_2 = 2$  or  $u_4 = 1$ .

(5)  $\dot{n} = 2, u_1 = n - 2 - 3u_3, u_2 = 1$  and  $u_3 \leq 2$ .

(6)  $\dot{n} = 0, u_3 \leq 4$ . In fact, if  $u_3 \geq 5$ , we have  $v(\tau_u) \geq v((2u_3 - 1)!) - v(u_3!) - 1 \geq 3$  since  $\dot{n} = 0$ . So for our purpose, we can assume that  $u_3 \leq 4$ .

For cases (1)–(3) and (4) with  $u_3 = 1$ , by the definition of  $\tau_u$ , we can easily check that  $v(\tau_u) \geq 3$ . We omit the details here.

For case (4) with  $u_3 = 0$ , if  $u_2 = 2$ , then

$$v(\tau_u) = v((2n - 4)!) - (n - 4) - v((n - 4)!) - v(2!) = 1 + v(n - 2) = 2 + v(n/2 - 1),$$

that is,  $\tau_u \equiv 0 \pmod 8$  for  $v(n) = 1$  and  $\tau_u \equiv 4 \pmod 8$  for  $v(n) \geq 2$ . If  $u_4 = 1$ , then

$$\tau_u = (-1)^{n-4}(2n - 5)! / (2^{n-4}(n - 4)!5) = 2(n - 3)(2n - 5)!! / 5 \equiv (-1)^{n/2} 2 \pmod 8.$$

For case (5), if  $u_3 = 2$ , then

$$v(\tau_u) = v((2n - 7)!) - (n - 4) - v((n - 8)!) - v(2!) = v((n - 4)(n - 6)) - 1.$$

Hence  $\tau_u \equiv 4 \pmod 8$  unless  $n \equiv 4$  or  $-2 \pmod 8$  where  $\tau_u \equiv 0 \pmod 8$ ; if  $u_3 = 1$ , then

$$\tau_u = (-1)^{n-4}(2n - 5)! / (2^{n-5}(n - 5)! \cdot 3 \cdot 4) = (n - 3)(n - 4)(2n - 5)!! / 3.$$

This implies that  $\tau_u \equiv 0 \pmod 8$  if  $v(n) = 2$ ,  $\tau_u \equiv 4 \pmod 8$  if  $v(n) > 2$ , and  $\tau_u \equiv -n \pmod 8$  if  $v(n) = 1$ ; if  $u_3 = 0$ , then

$$\tau_u = (-1)^{n-2}(2n - 3)! / (2^{n-2}(n - 2)! \cdot 3) = (2n - 3)!! / 3 \equiv 3(-1)^{n/2-1} \pmod 8.$$

For case (6), if  $u_3 = 4$ , then

$$\tau_u = (-1)^{n-9}(2n - 10)! / (2^{n-12+8}(n - 12)!4!) = -(n - 5) \cdots (n - 11)(2n - 11)!! / (2^4 3).$$

Therefore  $\tau_u \equiv 0 \pmod 4$  if  $v(n) = 1$  and  $\tau_u \equiv n/4 - 2 \pmod 8$  if  $v(n) \geq 2$ ; if  $u_3 = 3$ , then

$$\begin{aligned} v(\tau_u) &= v((2n - 8)!) - (n - 9 + 6) - v((n - 9)!) - v(3!) \\ &= v((n - 4)(n - 6)(n - 8)) - 2 \geq 3 \end{aligned}$$

unless  $n \equiv 2 \pmod 8$  where  $v(\tau_u) = 2$ ; if  $u_3 = 2$ , then we can derive that

$$\tau_u = -(2n - 6)! 2^{2-n} ((n - 6)!)^{-1} \cdot 2^{-1} = -(n - 3)(n - 4)(n - 5)(2n - 7)!! / 4.$$

So  $\tau_u \equiv 3(n - 4)/4 \pmod 4$  if  $v(n) = 1$  and  $\tau_u \equiv (n - 4)/4 \pmod 8$  if  $v(n) \geq 2$ ; if  $u_3 = 1$ , then

$$\tau_u = -(2n - 4)! 2^{1-n} ((n - 3)!)^{-1} = -(n - 2)(2n - 5)!! / 2.$$



Thus  $\tau_u \equiv -(n - 2)/2 \pmod 8$  if  $v(n) = 1$  and  $\tau_u \equiv -3(n - 2)/2 \pmod 8$  if  $v(n) \geq 2$ . If  $u_3 = 0$ , then  $\tau_u = -(2n - 3)/(2n)$ . By Lemma 4.1, we have  $\tau_u \equiv -1/(2n) \pmod 4$  if  $v(n) = 1$ . By Lemma 4.2(iii), we deduce that if  $v(n) = 2$ , then

$$\tau_u \equiv (2n)^{-1}(1 + (-1)^{(n+4)/8}16) \equiv 1/(2n) - 2 \pmod 8,$$

and if  $v(n) > 2$ , then

$$\tau_u \equiv (2n)^{-1}(1 + (-1)^{(n2^{-v(n)}-1)/2}2^{v(n)+2}) \equiv 1/(2n) + 2 \pmod 8$$

since  $(-1)^{(a-1)/2} \equiv a \pmod 4$  for any odd number  $a$ . So Theorem 5.1 is proved. □

With similar methods, but in a far more complicated fashion, we have also obtained the following theorem. For the sake of brevity we omit the proof.

**THEOREM 5.2.** *Let  $n = m + l$ ,  $l = k2^N$  with  $2 \nmid k$ . Let  $N \geq 3$  and  $m \geq 2N + 1$ .*

(i) *If  $2 \nmid m$ , then*

$$\begin{aligned} \hat{B}_n/n \equiv & c_1^l \hat{B}_m/m + l(c_1^{n-12}c_3^4 + c_1^{n-15}c_3^5 + c_1^{n-5}c_2c_3 + c_1^{n-8}c_2c_3^2 + c_1^{n-7}c_7) \\ & (-1)^{(m+1)/2}l(-c_1^n + c_1^{n-3}c_3 + c_1^{n-6}c_3^2 + c_1^{n-9}c_3^3)/2 \\ & \pmod{2^{N+1}\mathbf{Z}_2[c_1, \dots, c_n]}. \end{aligned}$$

(ii) *If  $2 \mid m$  and  $4 \nmid m$ , then*

$$\begin{aligned} \hat{B}_n/n \equiv & c_1^l \hat{B}_m/m + (l + l/(2mn))c_1^n + l(c_1^{n-9}c_3^3 + c_1^{n-18}c_3^6 + c_1^{n-5}c_2c_3 + c_1^{n-8}c_2c_3^2) \\ & - lc_1^{n-3}c_3/2 + 3lc_1^{n-6}c_3^2/4 + \theta c_1^{n-12}c_3^4 \pmod{2^{N+1}\mathbf{Z}_2[c_1, \dots, c_n]}, \end{aligned}$$

where  $\theta = -l/2$  for  $N = 3$  and  $\theta = l/2$  for  $N \geq 4$ .

(iii) *If  $4 \mid m$  and  $8 \nmid m$ , then*

$$\begin{aligned} \hat{B}_n/n \equiv & c_1^l \hat{B}_m/m + (l - l/(2mn))c_1^n + lc_1^{n-3}c_3/2 + l(c_1^{n-6}c_3^2 + c_1^{n-12}c_3^4)/4 \\ & + l(c_1^{n-8}c_2c_3^2 + c_1^{n-5}c_2c_3) \pmod{2^{N+1}\mathbf{Z}_2[c_1, \dots, c_n]}. \end{aligned}$$

(iv) *If  $8 \mid m$ , then*

$$\begin{aligned} \hat{B}_n/n \equiv & c_1^l \hat{B}_m/m - ((2n - 3)!/(2n) - (2m - 3)!/(2m))c_1^n \\ & + lc_1^{n-3}c_3/2 + 5lc_1^{n-12}c_3^4/4 + lc_1^{n-6}c_3^2/4 + l(c_1^{n-24}c_3^8 + c_1^{n-5}c_2c_3 \\ & + c_1^{n-8}c_2c_3^2) \pmod{2^{N+1}\mathbf{Z}_2[c_1, \dots, c_n]}. \end{aligned}$$

### Acknowledgements

The authors would like to thank Professor Shparlinski and the anonymous referee for their careful reading of the manuscript and for helpful comments and suggestions that improved its presentation.

## References

- [1] A. Adelberg, ‘Kummer congruences for universal Bernoulli numbers and related congruences for poly-Bernoulli numbers’, *Int. Math. J.* **1** (2002), 53–63.
- [2] A. Adelberg, ‘Universal Kummer congruences mod prime powers’, *J. Number Theory* **109** (2004), 362–378.
- [3] A. Adelberg, S. Hong and W. Ren, ‘Bounds of divided universal Bernoulli numbers and universal Kummer congruences’, *Proc. Amer. Math. Soc.* **136** (2008), 61–71.
- [4] A. Baker, F. Clarke, N. Ray and L. Schwartz, ‘On the Kummer congruences and the stable homotopy of BU’, *Trans. Amer. Math. Soc.* **316** (1989), 385–432.
- [5] F. Clarke, ‘The universal von Staudt theorem’, *Trans. Amer. Math. Soc.* **315** (1989), 591–603.
- [6] F. Clarke and C. Jones, ‘A congruence for factorials’, *Bull. Lond. Math. Soc.* **36** (2004), 553–558.
- [7] I. Dibag, ‘An analogue of the von Staudt–Clausen theorem’, *J. Algebra* **87** (1984), 332–341.
- [8] J. W. L. Glaisher, ‘On the residues of the sums of products of the first  $p - 1$  numbers, and their powers, to modulus  $p^2$  or  $p^3$ ’, *Quart. J. Pure Appl. Math.* **31** (1900), 321–353.
- [9] J. W. L. Glaisher, ‘On the residues of the inverse powers of numbers in arithmetic progression’, *Quart. J. Pure Appl. Math.* **32** (1901), 271–305.
- [10] S. Hong, ‘Notes on Glaisher’s congruences’, *Chinese Ann. Math.* **21B** (2000), 33–38.
- [11] A. Hurwitz, ‘Über die Entwicklungskoeffizienten der lemniskatischen Funktionen’, *Math. Ann.* **51** (1899), 196–226.
- [12] N. M. Katz, ‘The congruences of Clausen–von Staudt and Kummer for Bernoulli–Hurwitz numbers’, *Math. Ann.* **216** (1975), 1–4.
- [13] N. Koblitz, *p-Adic Numbers, p-adic Analysis, and Zeta-functions*, Graduate Texts in Mathematics, 58 (Springer, New York, 1984).
- [14] E. E. Kummer, ‘Über eine allgemeine Eigenschaft der rationalen Entwicklungskoeffizienten einer bestimmten Gattung analytischer Functionen’, *J. reine angew. Math.* **41** (1851), 368–372.
- [15] E. Lehmer, ‘On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson’, *Ann. of Math. (2)* **39** (1938), 350–360.
- [16] H. Miller, *Universal Bernoulli numbers and the  $S^1$ -transfer*, Canadian Mathematical Society Conference Proceedings, 2 (American Mathematical Society, Providence, RI, 1982), 437–449.
- [17] M. R. Murty, *Introduction to p-adic Analytic Number Theory*, Studies in Advanced Mathematics, 27 (American Math. Soc, Providence, RI, 2002).
- [18] N. Ray, ‘Extensions of umbral calculus I: Penumbral coalgebras and generalised Bernoulli numbers’, *Adv. Math.* **61** (1986), 41–100.
- [19] A. Robert, *A Course in p-adic Analysis*, Graduate Texts in Mathematics, 198 (Springer, New York, 2000).
- [20] P. Tempesta, ‘Formal groups, Bernoulli-type polynomials and L-series’, *C. R. Acad. Paris, Ser. I* **345** (2007), 303–306.
- [21] P. T. Young, ‘Congruences for Bernoulli, Euler and Stirling numbers’, *J. Number Theory* **78** (1999), 204–227.
- [22] P. T. Young, ‘Kummer congruences for values of Bernoulli and Euler polynomials’, *Acta Arith.* **99** (2001), 277–288.
- [23] J. Zhao, ‘Wolstenholme type theorem for multiple harmonic sums’, *Int. J. Number Theory* **4** (2008), 73–106.

SHAOFANG HONG, Yangtze Center of Mathematics, Sichuan University,  
Chengdu 610064, PR China

and

Mathematical College, Sichuan University,  
Chengdu 610064, PR China

e-mail: [sfhong@scu.edu.cn](mailto:sfhong@scu.edu.cn), [s-f.hong@tom.com](mailto:s-f.hong@tom.com), [hongsf02@yahoo.com](mailto:hongsf02@yahoo.com)

JIANRONG ZHAO, School of Economic Mathematics,  
Southwestern University of Finance and Economics,  
Chengdu 610074, PR China  
e-mail: [mathzjr@foxmail.com](mailto:mathzjr@foxmail.com)

WEI ZHAO, Science and Technology on Communication Security Laboratory,  
Chengdu 610041, PR China  
e-mail: [zhaowei9801@163.com](mailto:zhaowei9801@163.com)