ELSEVIER

Discrete Applied Mathematics 105 (2000) 193–223

DISCRETE APPLIED MATHEMATICS

Congruences concerning Bernoulli numbers and Bernoulli polynomials

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College, Huaiyin, Jiangsu 223001, The People's Republic of China

Abstract

Let $\{B_n(x)\}$ denote Bernoulli polynomials. In this paper we generalize Kummer's congruences by determining $B_{k(p-1)+b}(x)/(k(p-1)+b) \pmod{p^n}$, where p is an odd prime, x is a p-integral rational number and $p-1 \nmid b$. As applications we obtain explicit formulae for $\sum_{x=1}^{p-1}(1/x^k) \pmod{p^3}$, $\sum_{x=1}^{(p-1)/2}(1/x^k) \pmod{p^3}$, $(p-1)! \pmod{p^3}$ and $A_r(m,p) \pmod{p}$, where $k \in \{1,2,\ldots,p-1\}$ and $A_r(m,p)$ is the least positive solution of the congruence $px \equiv r \pmod{m}$. We also establish similar congruences for generalized Bernoulli numbers $\{B_{n,\chi}\}$.

1. Introduction

The Bernoulli numbers $\{B_n\}$ and Bernoulli polynomials $\{B_n(x)\}$ are defined as follows:

$$B_0 = 1, \quad \sum_{k=0}^{n-1} \binom{n}{k} B_k = 0 \quad (n = 2,3,4,\ldots),$$

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k} \quad (n = 0,1,2,\ldots).$$

Let p be an odd prime, and b an even number with $b \not\equiv 0 \pmod{p-1}$. In 1850 Kummer proved that [11]

$$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \frac{B_b}{b} \pmod{p} \quad \text{for } k = 0,1,2,\ldots .$$

This is now referred to as Kummer's congruences.

In this paper we show that

$$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv k\frac{B_{p-1+b}}{p-1+b} - (k-1)(1-p^{b-1})\frac{B_b}{b} \pmod{p^2} \tag{1.1}$$

E-mail address: hyzhsun@public.hy.js.cn (Z.-H. Sun).

0166-218X/00/$ - see front matter
PII: S0166-218X(00)00184-0

and

$$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \binom{k}{2}\frac{B_{2(p-1)+b}}{2(p-1)+b} - k(k-2)\frac{B_{p-1+b}}{p-1+b} + \binom{k-1}{2}(1-p^{b-1})\frac{B_b}{b} \pmod{p^3} \tag{1.2}$$

for $k = 1,2,3,\ldots$. Furthermore, we completely determine $B_{k(p-1)+b}(x)/(k(p-1)+b) \pmod{p^n}$ by proving that

$$\frac{B_{k(p-1)+b}(x) - p^{k(p-1)+b-1}B_{k(p-1)+b}\left(\frac{x+\langle -x\rangle_p}{p}\right)}{k(p-1)+b}$$
$$\equiv \sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r} \frac{B_{r(p-1)+b}(x) - p^{r(p-1)+b-1}B_{r(p-1)+b}\left(\frac{x+\langle -x\rangle_p}{p}\right)}{r(p-1)+b}$$
$$\equiv \sum_{r=0}^{n-1} a_r k^r \pmod{p^n} \quad (k = 0,1,2,\ldots),$$

where p is an odd prime, b is a positive integer with $b \not\equiv 0 \pmod{p-1}$, x is a p-integral rational number, $\langle -x\rangle_p$ is the least nonnegative residue of $-x \pmod p$, and $a_0,\ldots,a_{n-1}$ are all integers.

Clearly, the above result is a vast generalization of Kummer's congruences.

Let p be a prime greater than 3. In Section 5 we determine $\sum_{x=1}^{p-1}(1/x^k) \pmod{p^3}$ for $k = 1,2,\ldots,p-1$. In the cases $k = 1,2,\ldots,p-4$ our result is

$$\sum_{x=1}^{p-1}\frac{1}{x^k} \equiv \begin{cases} \binom{k+1}{2}\frac{B_{p-2-k}}{p-2-k}p^2 \pmod{p^3} & \text{if } k \text{ is odd,} \\ k\left(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k}\right)p \pmod{p^3} & \text{if } k \text{ is even.} \end{cases}$$

Taking $k = 1$ we find

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv -\frac{1}{3}p^2 B_{p-3} \pmod{p^3}.$$

This is stronger than the well-known congruence

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}.$$

In Section 5, we also determine $\sum_{x=1}^{(p-1)/2}(1/x^k) \pmod{p^3}$ for prime $p > 5$ and $k = 1,2,\ldots,p-4$. For example, if $q_p(2) = (2^{p-1}-1)/p$, then

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{(p-1)/2} \equiv -2q_p(2) + pq_p^2(2) - \frac{2}{3}p^2q_p^3(2) - \frac{7}{12}p^2 B_{p-3} \pmod{p^3}.$$

For prime $p > 3$, it is proved in Section 6 that

$$(p-1)! \equiv \frac{pB_{2p-2}}{2p-2} - \frac{pB_{p-1}}{p-1} - \frac{1}{2}\left(\frac{pB_{p-1}}{p-1}\right)^2 \pmod{p^3}.$$

This result is stronger than the known congruence $(p-1)! \equiv pB_{p-1} - p \pmod{p^2}$.

Let p be an odd prime, r an integer such that $0 < \langle r\rangle_{mp} < m + p$, and m a positive integer such that $p \nmid m$, and let $A_r(m,p)$ denote the least positive solution of the congruence $px \equiv r \pmod m$. In Section 7 we prove that

$$A_r(m,p) \equiv r - m\left[\frac{r}{mp}\right] + m\sum_{k=1}^{n}\binom{n}{k}(-1)^k\frac{B_{k(p-1)+1}(r/m)}{k(p-1)+1} \pmod{p^n}$$

provided $p > n$. Also,

$$A_r(m,p) \equiv r - m\left[\frac{r}{mp}\right] - \frac{m}{2} - \frac{1}{p^2}\sum_{k=0}^{p-1}(km+r)^p \pmod p.$$

As a consequence we obtain

$$\frac{(p-1)!+1}{p} \equiv \frac{1}{2}\sum_{m=1}^{p-1}A_1(m,p) \pmod p.$$

The purpose of Section 8 is to establish the congruences for $pB_{k(p-1)+b,\chi} \pmod{p^n}$, where p is a prime, b is a nonnegative integer and χ is a Dirichlet character modulo m ($m \not\equiv 0 \pmod p$).

For later convenience we introduce the following notations: $\mathbb{Z}$ — the set of integers, $\mathbb{Z}^+$ — the set of positive integers, $\mathbb{Z}_p$ — the set of those rational numbers whose denominator is prime to p, $\langle x\rangle_p$ — the least nonnegative residue of x modulo p, $[x]$ — the greatest integer not exceeding x, $\varphi(m)$ — Euler's totient function.

2. p-regular functions

In this section we introduce the notion of p-regular functions and investigate their properties.

Definition 2.1. Let p be a prime. If $f(k) \in \mathbb{Z}_p$ for any $k \in \mathbb{Z}^+ \cup \{0\}$ and

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k f(k) \equiv 0 \pmod{p^n} \quad \text{for} \quad n = 1,2,3,\ldots,$$

then f is called a p-regular function.

For example, it follows from Fermat's little theorem that both $m^{k(p-1)+b}$ and $m^{k(p-1)+b}-1$ are p-regular functions, where $m\in\mathbb{Z}^+$, $m\not\equiv 0 \pmod p$ and $b\in\mathbb{Z}^+\cup\{0\}$.

We mention that Gillespie [7] has introduced the so-called e_n-sequences which are related to p-regular functions.

Theorem 2.1. *Let p be a prime.*
(a) *If f is a p-regular function, then for each positive integer n there are $a_0,\dots,a_{n-1}\in\mathbb{Z}_p$ satisfying the following conditions*:
(i) $f(k)\equiv a_{n-1}k^{n-1}+\cdots+a_1k+a_0 \pmod{p^n}\quad (k=0,1,2,\dots)$,
(ii) $a_s\cdot s!/p^s\in\mathbb{Z}_p\quad (s=0,1,\dots,n-1)$.

Furthermore, if $p\geqslant n$ then $a_0,\dots,a_{n-1} \pmod{p^n}$ are uniquely determined by (i).
(b) *If for any given positive integer n there are $a_0,a_1,\dots,a_{n-1}\in\mathbb{Z}_p$ such that*

$$f(k)\equiv a_{n-1}k^{n-1}+\cdots+a_1k+a_0 \pmod{p^n}\quad \textit{for } k=0,1,\dots,n,$$

then f is a p-regular function.

Proof. Suppose that f is a p-regular function and $A_k=(1/p^k)\sum_{r=0}^{k}\binom{k}{r}(-1)^r f(r)$. Then $A_k\in\mathbb{Z}_p$ for $k\geqslant 0$. Hence, applying the binomial inversion formula we obtain

$$f(k)=\sum_{r=0}^{k}\binom{k}{r}(-1)^r p^r A_r\equiv\sum_{r=0}^{n-1}\binom{k}{r}(-1)^r p^r A_r \pmod{p^n}.$$

Let $\{s(n,k)\}$ be the Stirling numbers of the first kind given by

$$x(x-1)\cdots(x-n+1)=\sum_{k=0}^{n}(-1)^{n-k}s(n,k)x^k.$$

It is well known that [2, (5.5.2)]

$$\frac{\log^m(1+x)}{m!}=\sum_{n=m}^{\infty}(-1)^{n-m}s(n,m)\frac{x^n}{n!}.$$

Since

$$\log^m(1+x)$$
$$=\left(\sum_{k=1}^{\infty}\frac{(-1)^{k-1}}{k}x^k\right)^m$$
$$=\sum_{n=m}^{\infty}\left(\sum_{\substack{k_1+k_2+\cdots+k_n=m\\ k_1+2k_2+\cdots+nk_n=n}}\frac{(k_1+k_2+\cdots+k_n)!}{k_1!k_2!\cdots k_n!}\prod_{r=1}^{n}\left(\frac{(-1)^{r-1}}{r}\right)^{k_r}\right)x^n,$$

we find

$$s(n,m)=\sum_{\substack{k_1+k_2+\cdots+k_m=m\\ k_1+2k_2+\cdots+nk_n=n}}\frac{n!}{1^{k_1}k_1!\cdots n^{k_n}k_n!}.$$

Thus,

$$\frac{s(n,m)m!}{n!}p^{n-m} = \sum_{\substack{k_1+k_2+\cdots+k_n=m \\ k_1+2k_2+\cdots+nk_n=n}} \frac{(k_1+k_2+\cdots+k_n)!}{k_1!k_2!\cdots k_n!} \prod_{r=1}^{n} \left(\frac{p^{r-1}}{r}\right)^{k_r}.$$

Observing that $p^{r-1}/r \in \mathbb{Z}_p$ for $r \geqslant 1$ we get

$$\frac{s(n,m)m!}{n!}p^{n-m} \in \mathbb{Z}_p. \tag{2.1}$$

Now, by the above,

$$f(k) \equiv \sum_{r=0}^{n-1} \binom{k}{r}(-p)^r A_r = A_0 + \sum_{r=1}^{n-1}\left(\sum_{s=1}^{r}(-1)^{r-s}s(r,s)k^s\right)\frac{(-p)^r}{r!}A_r$$

$$= A_0 + \sum_{s=1}^{n-1}\left(\sum_{r=s}^{n-1} s(r,s)\frac{p^r}{r!}A_r\right)(-k)^s = \sum_{s=0}^{n-1} a_s k^s \pmod{p^n},$$

where $a_0 = A_0$ and

$$a_s = (-1)^s \sum_{r=s}^{n-1} s(r,s)\frac{p^r}{r!}A_r \quad \text{for } s = 1,2,\ldots,n-1.$$

Since $p^r/r! \in \mathbb{Z}_p$ and $A_r \in \mathbb{Z}_p$ we must have $a_s \in \mathbb{Z}_p$ for $s = 0,1,\ldots,n-1$. In view of (2.1) we obtain

$$\frac{a_s s!}{p^s} = (-1)^s \sum_{r=s}^{n-1} \frac{s(r,s)s!}{r!} p^{r-s} A_r \in \mathbb{Z}_p \quad \text{for } s = 0,1,\ldots,n-1.$$

Now assume $p \geqslant n$ and

$$f(k) \equiv \sum_{r=0}^{n-1} a_r k^r \equiv \sum_{r=0}^{n-1} b_r k^r \pmod{p^n} \quad \text{for } k = 0,1,2,\ldots .$$

For $r \in \{0,1,\ldots,m\}$ Euler's identity states that [18,20]

$$\sum_{k=0}^{m} \binom{m}{k}(-1)^{m-k}k^r = \begin{cases} m! & \text{if } r = m, \\ 0 & \text{if } r < m. \end{cases} \tag{2.2}$$

Thus, for $m = 0,1,\ldots,n-1$ we have

$$(a_m - b_m)m! = \sum_{k=0}^{m} \binom{m}{k}(-1)^{m-k}\left(\sum_{r=0}^{m}(a_r - b_r)k^r\right).$$

Note that $m \leqslant n-1 \leqslant p-1$ and so $p \nmid m!$. From the above we see that $\sum_{r=0}^{m}(a_r - b_r)k^r \equiv 0 \pmod{p^n}$ $(k = 0,1,2,\ldots)$ implies that $a_m \equiv b_m \pmod{p^n}$ and so $\sum_{r=0}^{m-1}(a_r - b_r)k^r \equiv 0 \pmod{p^n}$ $(k = 0,1,2,\ldots)$. Putting this together with the assumption that $\sum_{r=0}^{n-1}(a_r - b_r)k^r \equiv 0 \pmod{p^n}$ $(k = 0,1,2,\ldots)$ yields

$$a_{n-1} - b_{n-1} \equiv \cdots \equiv a_0 - b_0 \equiv 0 \pmod{p^n}.$$

Finally, if $f(k)\equiv\sum_{r=0}^{n-1}a_rk^r\ (\mathrm{mod}\ p^n)$ for $k=0,1,\dots,n$, by (2.2) we find

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^kf(k)\equiv\sum_{r=0}^{n-1}\left(\sum_{k=0}^{n}\binom{n}{k}(-1)^kk^r\right)a_r=0\ (\mathrm{mod}\ p^n).$$

Now, combining the above we prove the theorem.

Corollary 2.1. *Let p be a prime, and f a p-regular function. Then $f(kp^{n-1})\equiv f(0)\ (\mathrm{mod}\ p^n)$ for any positive integers k and n.*

Proof. It follows from Theorem 2.1 that there are $a_0,\dots,a_{n-1}\in\mathbb{Z}_p$ satisfying $f(r)\equiv\sum_{s=0}^{n-1}a_sr^s\ (\mathrm{mod}\ p^n)$ for $r=0,1,2,\dots$ and $a_ss!/p^s\in\mathbb{Z}_p$ for $s=0,1,\dots,n-1$. Since $p^{s-1}/s!\in\mathbb{Z}_p$ for $s\geqslant1$ we must have $a_s\equiv0\ (\mathrm{mod}\ p)$ for $s\geqslant1$ and therefore

$$f(kp^{n-1})\equiv\sum_{s=0}^{n-1}a_s(kp^{n-1})^s\equiv a_0\equiv f(0)\ (\mathrm{mod}\ p^n).$$

This proves the corollary.

Remark 2.1. Using the properties of Stirling numbers we can prove the following general congruence:

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^kf(kp^{m-1}t)\equiv0\ (\mathrm{mod}\ p^{mn}),\tag{2.3}$$

where p is a prime, f is a p-regular function, and $m,n,t\in\mathbb{Z}^+$.

Theorem 2.2. *Let p be a prime, $n\in\mathbb{Z}^+$, $k\in\mathbb{Z}^+\cup\{0\}$, and f a p-regular function. Then*

$$f(k)\equiv\sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r}f(r)\ (\mathrm{mod}\ p^n).$$

Proof. This is immediate from [17, Lemma 2.1].

Remark 2.2. From [17, Lemma 2.1] and (2.3) we have the following generalization of Theorem 2.2:

Let p be a prime, $m,n\in\mathbb{Z}^+$, $k,t\in\mathbb{Z}^+\cup\{0\}$, and f a p-regular function. Then

$$f(kp^{m-1}t)\equiv\sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r}f(rp^{m-1}t)\ (\mathrm{mod}\ p^{mn}).\tag{2.4}$$

Lemma 2.1. *For $n=0,1,2,\dots$ and any two functions f and g we have*

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^kf(k)g(k)=\sum_{s=0}^{n}\binom{n}{s}\left(\sum_{r=0}^{s}\binom{s}{r}(-1)^rF(n-s+r)\right)G(s),$$

where

$$F(m)=\sum_{k=0}^{m}\binom{m}{k}(-1)^k f(k)\quad\text{and}\quad G(m)=\sum_{k=0}^{m}\binom{m}{k}(-1)^k g(k).$$

Proof. We first claim that

$$\sum_{r=0}^{n}\binom{n}{r}(-1)^r f(r+m)=\sum_{r=0}^{m}\binom{m}{r}(-1)^r F(r+n). \tag{2.5}$$

Clearly, the assertion holds for $m=0$. Now assume that it is true for $m=k$. It is easily seen that

$$\begin{aligned}&\sum_{r=0}^{n}\binom{n}{r}(-1)^r f(r+k+1)\\ &\quad=\sum_{s=0}^{n}\binom{n}{s}(-1)^s f(k+s)-\sum_{s=0}^{n+1}\binom{n+1}{s}(-1)^s f(k+s)\\ &\quad=\sum_{s=0}^{k}\binom{k}{s}(-1)^s F(n+s)-\sum_{s=0}^{k}\binom{k}{s}(-1)^s F(n+1+s)\\ &\quad=\sum_{s=0}^{k+1}\binom{k+1}{s}(-1)^s F(n+s).\end{aligned}$$

So the assertion is true by induction.

From the binomial inversion formula we know that $g(k)=\sum_{s=0}^{k}\binom{k}{s}(-1)^s G(s)$. Thus, by the above assertion we have

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}(-1)^k f(k)g(k)&=\sum_{k=0}^{n}\binom{n}{k}(-1)^k f(k)\sum_{s=0}^{k}\binom{k}{s}(-1)^s G(s)\\ &=\sum_{s=0}^{n}\left(\sum_{k=s}^{n}\binom{n}{k}\binom{k}{s}(-1)^{k-s}f(k)\right)G(s)\\ &=\sum_{s=0}^{n}\binom{n}{s}\left(\sum_{k=s}^{n}\binom{n-s}{k-s}(-1)^{k-s}f(k)\right)G(s)\\ &=\sum_{s=0}^{n}\binom{n}{s}\left(\sum_{r=0}^{n-s}\binom{n-s}{r}(-1)^r f(r+s)\right)G(s)\\ &=\sum_{s=0}^{n}\binom{n}{s}\left(\sum_{r=0}^{s}\binom{s}{r}(-1)^r F(n-s+r)\right)G(s),\end{aligned}$$

which completes the proof. □

Theorem 2.3 (Product Theorem). *Let p be a prime. If f and g are p-regular functions, then $f \cdot g$ is also a p-regular function.*

Proof. This is immediate from Lemma 2.1 and Definition 2.1.

3. The Kummer type congruences

In this section we mainly generalize the following Kummer's congruences [11,15]:

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k \frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv 0 \pmod{p^n},$$

where p is an odd prime, $b > n \geqslant 1$ and $b \not\equiv 0 \pmod{p-1}$.

Lemma 3.1. *Suppose that $p > 1$ is odd and $k \in \mathbb{Z}^+$. If $x, x_0 \in \mathbb{Z}_p$ and $x \equiv x_0 \pmod p$ then*

$$\frac{B_k(x) - B_k(x_0)}{k} \equiv (x - x_0) B_{k-1} \pmod p.$$

Proof. It is well known that $B_k(x_1 + x_2) = \sum_{r=0}^{k} \binom{k}{r} B_{k-r}(x_1) x_2^r$. Thus,

$$\begin{aligned}
\frac{B_k(x) - B_k(x_0)}{k} &= \frac{1}{k} \sum_{r=1}^{k} \binom{k}{r} B_{k-r}(x_0)(x - x_0)^r \\
&= \sum_{r=1}^{k} \binom{k-1}{r-1} (B_{k-r}(x_0) - B_{k-r} + B_{k-r}) \frac{p^r}{r} \left(\frac{x - x_0}{p}\right)^r \\
&\equiv \sum_{r=1}^{k} \binom{k-1}{r-1} pB_{k-r} \frac{p^{r-1}}{r} \left(\frac{x - x_0}{p}\right)^r \\
&\quad \text{(note that } p^{r-1}/r \in \mathbb{Z}_p \text{ and that } B_{k-r}(x_0) - B_{k-r} \in \mathbb{Z}_p \\
&\quad \quad \text{by [17, Lemma 2.3])} \\
&\equiv pB_{k-1} \frac{x - x_0}{p} \pmod p \\
&\quad \text{(note that } p^{r-2}/r \in \mathbb{Z}_p \text{ for } r \geqslant 2 \text{ and } pB_{k-r} \in \mathbb{Z}_p \\
&\quad \quad \text{by [17, Lemma 2.3]).}
\end{aligned}$$

So the lemma is proved.

Lemma 3.2. *If* $p>1$ *is odd,* $k\in\mathbb{Z}^+\cup\{0\}$ *and* $x\in\mathbb{Z}_p$, *then*

$$(-1)^{k+1}\frac{B_{k+1}(x)-B_{k+1}}{k+1}\equiv\sum_{r=1}^{\langle -x\rangle_p} r^k-(x+\langle -x\rangle_p)B_k \pmod p.$$

Proof. Clearly,

$$B_1-B_1(x)=-x=\langle -x\rangle_p-(x+\langle -x\rangle_p)B_0.$$

So the result is true for $k=0$.

Now assume $k>0$. Notice that $B_{2n+1}=0$ for $n\geqslant 1$ and $B_m(1-x)=(-1)^m B_m(x)$. Applying Lemma 3.1 we find

$$\begin{aligned}\sum_{r=0}^{\langle -x\rangle_p} r^k&=\frac{B_{k+1}(1+\langle -x\rangle_p)-B_{k+1}}{k+1}\\&=\frac{B_{k+1}(x+\langle -x\rangle_p+1-x)-B_{k+1}(1-x)}{k+1}+\frac{B_{k+1}(1-x)-B_{k+1}}{k+1}\\&\equiv(x+\langle -x\rangle_p)B_k+(-1)^{k+1}\frac{B_{k+1}(x)-B_{k+1}}{k+1} \pmod p.\end{aligned}$$

This is the result.

We are now able to give

Theorem 3.1. *Let* p *be an odd prime,* $b\in\mathbb{Z}^+$ *and* $x\in\mathbb{Z}_p$. *For* $n=1,2,3,\ldots$ *we have*

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k\left(\frac{B_{k(p-1)+b}(x)-B_{k(p-1)+b}}{k(p-1)+b}\right.$$
$$\left.-p^{k(p-1)+b-1}\frac{B_{k(p-1)+b}\left(\frac{x+\langle -x\rangle_p}{p}\right)-B_{k(p-1)+b}}{k(p-1)+b}\right)\equiv 0 \pmod{p^n}.$$

Proof. By Lemma 3.2,

$$\begin{aligned}&(-1)^b\frac{B_{k(p-1)+b}(x)-B_{k(p-1)+b}}{k(p-1)+b}\\&\quad\equiv\sum_{r=1}^{\langle -x\rangle_{p^n}} r^{k(p-1)+b-1}-(x+\langle -x\rangle_{p^n})B_{k(p-1)+b-1} \pmod{p^n}.\end{aligned}$$

Observing that

$$\langle -x\rangle_{p^n}-\langle -x\rangle_p=\langle -x-\langle -x\rangle_p\rangle_{p^n}=p\left\langle -\frac{x+\langle -x\rangle_p}{p}\right\rangle_{p^{n-1}}$$

and so

$$\frac{x+\langle -x\rangle_p}{p}+\left\langle -\frac{x+\langle -x\rangle_p}{p}\right\rangle_{p^{n-1}}=\frac{x+\langle -x\rangle_{p^n}}{p},$$

we obtain

$$(-1)^b p^{k(p-1)+b-1}\frac{B_{k(p-1)+b}\left(\frac{x+\langle -x\rangle_p}{p}\right)-B_{k(p-1)+b}}{k(p-1)+b}$$

$$\equiv p^{k(p-1)+b-1}\left(\sum_{s=1}^{\left\langle -\frac{x+\langle -x\rangle_p}{p}\right\rangle_{p^{n-1}}} s^{k(p-1)+b-1}-\frac{x+\langle -x\rangle_{p^n}}{p}B_{k(p-1)+b-1}\right)$$

$$=\sum_{s=1}^{\frac{\langle -x\rangle_{p^n}-\langle -x\rangle_p}{p}}(sp)^{k(p-1)+b-1}-p^{k(p-1)+b-2}(x+\langle -x\rangle_{p^n})B_{k(p-1)+b-1}$$

$$=\sum_{\substack{r=1\\ p\mid r}}^{\langle -x\rangle_{p^n}} r^{k(p-1)+b-1}-p^{k(p-1)+b-2}(x+\langle -x\rangle_{p^n})B_{k(p-1)+b-1} \pmod{p^n}$$

and therefore

$$(-1)^b\sum_{k=0}^{n}\binom{n}{k}(-1)^k\left(\frac{B_{k(p-1)+b}(x)-B_{k(p-1)+b}}{k(p-1)+b}\right.$$

$$\left.-p^{k(p-1)+b-1}\frac{B_{k(p-1)+b}\left(\frac{x+\langle -x\rangle_p}{p}\right)-B_{k(p-1)+b}}{k(p-1)+b}\right)$$

$$\equiv\sum_{k=0}^{n}\binom{n}{k}(-1)^k\left(\sum_{r=1}^{\langle -x\rangle_{p^n}} r^{k(p-1)+b-1}-\sum_{\substack{r=1\\ p\mid r}}^{\langle -x\rangle_{p^n}} r^{k(p-1)+b-1}\right.$$

$$\left.+(p^{k(p-1)+b-2}-1)(x+\langle -x\rangle_{p^n})B_{k(p-1)+b-1}\right)$$

$$=\sum_{\substack{r=1\\ p\nmid r}}^{\langle -x\rangle_{p^n}} r^{b-1}(1-r^{p-1})^n$$

$$+(x+\langle -x\rangle_{p^n})\sum_{k=0}^{n}\binom{n}{k}(-1)^k(p^{k(p-1)+b-2}-1)B_{k(p-1)+b-1}$$

$$\equiv\frac{x+\langle -x\rangle_{p^n}}{p^n}\cdot p^{n-1}\left((p^{b-1}-p)B_{b-1}\right.$$

$$\left.-\sum_{k=1}^{n}\binom{n}{k}(-1)^k pB_{k(p-1)+b-1}\right) \pmod{p^n}$$

(by using Fermat's little theorem).

To complete the proof, we note that

$$pB_{k(p-1)+b-1} \equiv \begin{cases} 0 \pmod p & \text{if } p-1 \nmid b-1 \text{ or } k(p-1)+b-1=0, \\ -1 \pmod p & \text{if } p-1 \mid b-1 \text{ and } k(p-1)+b-1>0 \end{cases}$$

and therefore that

$$\sum_{k=1}^{n} \binom{n}{k} (-1)^k pB_{k(p-1)+b-1} \equiv (p^{b-1}-p)B_{b-1} \pmod p.$$

Remark 3.1. In a similar way one can prove that the result of Theorem 3.1 is also true for $p=2$.

Now we can give the following generalization of Kummer's congruences.

Theorem 3.2. *Let p be an odd prime, $n,b \in \mathbb{Z}^+$, $x \in \mathbb{Z}_p$ and $p-1 \nmid b$. Then*

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k \frac{B_{k(p-1)+b}(x) - p^{k(p-1)+b-1} B_{k(p-1)+b}\left(\frac{x+\langle -x\rangle_p}{p}\right)}{k(p-1)+b} \equiv 0 \pmod{p^n}.$$

Proof. Suppose $m \in \mathbb{Z}^+$ and $m \not\equiv 0 \pmod p$. For $r \in \{0,1,\ldots,m-1\}$ let $A'_r(m,p)$ denote the least nonnegative solution of the congruence $px \equiv r \pmod m$. It is obvious that

$$\left\langle -\frac{r}{m} \right\rangle_p = \frac{pA'_r(m,p)-r}{m} \quad \text{and so} \quad \frac{r/m + \langle -r/m\rangle_p}{p} = \frac{A'_r(m,p)}{m}.$$

Set

$$f_r(k) = \frac{B_{k(p-1)+b}(r/m) - B_{k(p-1)+b}}{k(p-1)+b} - p^{k(p-1)+b-1} \frac{B_{k(p-1)+b}\left(\frac{A'_r(m,p)}{m}\right) - B_{k(p-1)+b}}{k(p-1)+b}.$$

By the fact that $\{A'_0(m,p), A'_1(m,p), \ldots, A'_{m-1}(m,p)\} = \{0,1,\ldots,m-1\}$ and Raabe's theorem [17, Lemma 2.2] we get

$$\sum_{r=0}^{m-1} f_r(k) = (1-p^{k(p-1)+b-1}) \frac{\sum_{r=0}^{m-1} B_{k(p-1)+b}(r/m) - mB_{k(p-1)+b}}{k(p-1)+b}$$

$$= (1-p^{k(p-1)+b-1})(m^{-(k(p-1)+b-1)} - m) \frac{B_{k(p-1)+b}}{k(p-1)+b}.$$

Putting this together with Theorem 3.1 yields

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k (1-p^{k(p-1)+b-1})(m^{-(k(p-1)+b)} - 1) \frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv 0 \pmod{p^n}. \tag{3.1}$$

Let $g \in \{1, 2, \ldots, p-1\}$ be a primitive root of p. Then $g^{p^{n-1}(p-1)} \equiv 1 \pmod{p^n}$ and $g^{p^{n-1}b} \not\equiv 1 \pmod{p}$. Taking $m = g^{p^{n-1}}$ in (3.1) we find

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k (g^{-p^{n-1}b} - 1)(1 - p^{k(p-1)+b-1}) \frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv 0 \pmod{p^n}$$

and hence

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k (1 - p^{k(p-1)+b-1}) \frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv 0 \pmod{p^n}.$$

Combining this with Theorem 3.1 gives the result.

Corollary 3.1. *Let p be an odd prime, $k, n, b \in \mathbb{Z}^+$, $p-1 \nmid b$ and $x \in \mathbb{Z}_p$. Then*

$$\frac{B_{k\varphi(p^n)+b}(x)}{k\varphi(p^n)+b} \equiv \frac{B_b(x) - p^{b-1} B_b\left(\frac{x+\langle -x\rangle_p}{p}\right)}{b} \pmod{p^n}.$$

Proof. This is immediate from Theorem 3.2 and Corollary 2.1.

We remark that the special case $x = 0$ of Corollary 3.1 is known as Kummer's congruences [11,20].

4. Congruences for $B_{k(p-1)+b}(x) \pmod{p^n}$

This section is devoted to determining $B_{k(p-1)+b}(x)/(k(p-1)+b) \pmod{p^n}$, where p is an odd prime, $x \in \mathbb{Z}_p$ and $b \not\equiv 0 \pmod{p-1}$.

Theorem 4.1. *Let p be an odd prime, $n, b \in \mathbb{Z}^+$, $p-1 \nmid b$ and $x \in \mathbb{Z}_p$. Then there are n integers $a_0, \ldots, a_{n-1}$ such that $a_s s!/p^s \in \mathbb{Z}_p$ $(s = 0, 1, \ldots, n-1)$ and*

$$\frac{B_{k(p-1)+b}(x) - p^{k(p-1)+b-1} B_{k(p-1)+b}(\frac{x+\langle -x\rangle_p}{p})}{k(p-1)+b}$$
$$\equiv a_{n-1}k^{n-1} + \cdots + a_1 k + a_0 \pmod{p^n}$$

for every $k = 0, 1, 2, \ldots$. Moreover, if $p \geqslant n$ then $a_0, \ldots, a_{n-1} \pmod{p^n}$ are uniquely determined by the above congruences.

Proof. This is immediate from Theorems 2.1 and 3.2.

As an example, we point out the following congruence:

$$(1 - 5^{4k+1}) \frac{B_{4k+2}}{4k+2} \equiv 625k^4 + 875k^3 - 700k^2 + 180k - 1042 \pmod{5^5}. \qquad (4.1)$$

Theorem 4.2. *Let p be an odd prime, $k\in\mathbb{Z}^+\cup\{0\}$, or $n,b\in\mathbb{Z}^+$, $p-1\nmid b$ and $x\in\mathbb{Z}_p$. Then*

$$\frac{B_{k(p-1)+b}(x)-p^{k(p-1)+b-1}B_{k(p-1)+b}\left(\frac{x+\langle -x\rangle_p}{p}\right)}{k(p-1)+b}$$

$$\equiv\sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r}$$

$$\frac{B_{r(p-1)+b}(x)-p^{r(p-1)+b-1}B_{r(p-1)+b}\left(\frac{x+\langle -x\rangle_p}{p}\right)}{r(p-1)+b}\pmod{p^n}.$$

Proof. This is immediate from Theorems 2.2 and 3.2.

Corollary 4.1. *Let p be an odd prime, $k\in\mathbb{Z}^+\cup\{0\}$, $n,b\in\mathbb{Z}^+$ and $p-1\nmid b$. Then*

$$(1-p^{k(p-1)+b-1})\frac{B_{k(p-1)+b}}{k(p-1)+b}$$

$$\equiv\sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r}(1-p^{r(p-1)+b-1})\frac{B_{r(p-1)+b}}{r(p-1)+b}\pmod{p^n}.$$

Clearly, taking $n=2,3$ in Corollary 4.1 gives (1.1) and (1.2).

5. Congruences for $\sum_{x=1}^{p-1}(1/x^k)\pmod{p^3}$ and $\sum_{x=1}^{(p-1)/2}(1/x^k)\pmod{p^3}$

Theorem 5.1. *Let p be a prime greater than 3.*

(a) *If $k\in\{1,2,\ldots,p-4\}$ then*

$$\sum_{x=1}^{p-1}\frac{1}{x^k}\equiv\begin{cases}\frac{k(k+1)}{2}\frac{B_{p-2-k}}{p-2-k}p^2\pmod{p^3} & \text{if } k \text{ is odd},\\ k\left(\frac{B_{2p-2-k}}{2p-2-k}-2\frac{B_{p-1-k}}{p-1-k}\right)p\pmod{p^3} & \text{if } k \text{ is even}.\end{cases}$$

(b)

$$\sum_{x=1}^{p-1}\frac{1}{x^{p-3}}\equiv\left(\frac{1}{2}-3B_{p+1}\right)p-\frac{4}{3}p^2\pmod{p^3}.$$

(c)

$$\sum_{x=1}^{p-1}\frac{1}{x^{p-2}}\equiv-(2+pB_{p-1})p+\frac{5}{2}p^2\pmod{p^3}.$$

(d)

$$\sum_{x=1}^{p-1}\frac{1}{x^{p-1}}\equiv pB_{2p-2}-3pB_{p-1}+3(p-1)\pmod{p^3}.$$

Proof. For $m \in \mathbb{Z}^+$ it is clear that

$$\begin{aligned}1^m + 2^m + \cdots + (p-1)^m &= \frac{B_{m+1}(p) - B_{m+1}}{m+1} \\ &= \frac{1}{m+1}\sum_{r=1}^{m+1}\binom{m+1}{r} B_{m+1-r}\, p^r \\ &= pB_m + \frac{p^2}{2} mB_{m-1} + \frac{p^3}{6} m(m-1)B_{m-2} \\ &\quad + \sum_{r=4}^{m+1}\binom{m}{r-1} pB_{m+1-r}\frac{p^{r-4}}{r} p^3.\end{aligned}$$

Since $pB_{m+1-r}, p^{r-4}/r \in \mathbb{Z}_p$ for $r \geqslant 4$ we have

$$1^m + 2^m + \cdots + (p-1)^m \equiv pB_m + \frac{p^2}{2} mB_{m-1} + \frac{p^3}{6} m(m-1)B_{m-2} \pmod{p^3}. \tag{5.1}$$

Let $k \in \{1, 2, \ldots, p-1\}$. From (5.1) and Euler's theorem we see that

$$\begin{aligned}\sum_{x=1}^{p-1}\frac{1}{x^k} &\equiv \sum_{x=1}^{p-1} x^{\varphi(p^3)-k} \equiv pB_{\varphi(p^3)-k} + \frac{p^2}{2}(\varphi(p^3)-k)B_{\varphi(p^3)-k-1} \\ &\quad + \frac{p^3}{6}(\varphi(p^3)-k)(\varphi(p^3)-k-1)B_{\varphi(p^3)-k-2} \\ &\equiv pB_{\varphi(p^3)-k} - \frac{k}{2}p^2 B_{\varphi(p^3)-k-1} + \tfrac{k(k+1)}{6} p^3 B_{\varphi(p^3)-k-2} \\ &\equiv \begin{cases} pB_{\varphi(p^3)-k} + \frac{k(k+1)}{6} p^3 B_{\varphi(p^3)-k-2} \pmod{p^3} & \text{if } k \text{ is even,} \\ -\frac{k}{2} p^2 B_{\varphi(p^3)-k-1} \pmod{p^3} & \text{if } k \text{ is odd.}\end{cases}\end{aligned}$$

For $k \in \{1, 2, \ldots, p-2\}$ it follows from Corollary 4.1 or (1.1) that

$$\begin{aligned}\frac{B_{\varphi(p^3)-k}}{\varphi(p^3)-k} &= \frac{B_{(p^2-1)(p-1)+p-1-k}}{(p^2-1)(p-1)+p-1-k} \\ &\equiv (p^2-1)\frac{B_{2p-2-k}}{2p-2-k} - (p^2-2)(1-p^{p-2-k})\frac{B_{p-1-k}}{p-1-k} \\ &\equiv -\frac{B_{2p-2-k}}{2p-2-k} + 2(1-p^{p-2-k})\frac{B_{p-1-k}}{p-1-k} \pmod{p^2}.\end{aligned}$$

Thus,

$$\begin{aligned}pB_{\varphi(p^3)-k} &\equiv -kp\left(-\frac{B_{2p-2-k}}{2p-2-k} + 2(1-p^{p-2-k})\frac{B_{p-1-k}}{p-1-k}\right) \\ &\equiv \begin{cases} kp\left(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k}\right) \pmod{p^3} & \text{if } k < p-3, \\ (p-3)p\left(\frac{B_{p+1}}{p+1} - 2(1-p)\frac{B_2}{2}\right) \pmod{p^3} & \text{if } k = p-3.\end{cases}\end{aligned} \tag{5.2}$$

When $k\in\{1,2,\dots,p-3\}$, it follows from Kummer's congruences that

$$\frac{B_{\varphi(p^3)-k-1}}{\varphi(p^3)-k-1}=\frac{B_{(p^2-1)(p-1)+p-2-k}}{(p^2-1)(p-1)+p-2-k}\equiv\frac{B_{p-2-k}}{p-2-k}\pmod p.$$

Thus,

$$-\frac{k}{2}p^2B_{\varphi(p^3)-k-1}\equiv-\frac{k}{2}p^2(-k-1)\frac{B_{p-2-k}}{p-2-k}\pmod{p^3}.\tag{5.3}$$

Combining the above we get

$$\sum_{x=1}^{p-1}\frac{1}{x^k}\equiv\begin{cases}kp\left(\frac{B_{2p-2-k}}{2p-2-k}-2\frac{B_{p-1-k}}{p-1-k}\right)\pmod{p^3} & \text{if } k\in\{2,4,\dots,p-5\},\\ \left(\frac12-3B_{p+1}\right)p-\frac43p^2\pmod{p^3} & \text{if } k=p-3,\\ \frac{k(k+1)}{2}\frac{B_{p-2-k}}{p-2-k}p^2\pmod{p^3} & \text{if } k\in\{1,3,\dots,p-4\}.\end{cases}$$

This proves parts (a) and (b).

Now consider parts (c) and (d). Note that $pB_{r(p-1)}\equiv-1\pmod p$ for $r\geqslant1$. From the above and [17, Corollary 4.2] we see that

$$\begin{aligned}\sum_{x=1}^{p-1}\frac{1}{x^{p-2}}&\equiv-\frac{p-2}{2}p^2B_{\varphi(p^3)-(p-1)}\\&\equiv-\frac{p-2}{2}p((p^2-1)pB_{p-1}-(p^2-2)(p-1))\\&\equiv\frac{p-2}{2}p(pB_{p-1}+2-2p)\equiv-p(pB_{p-1}+2)+\frac52p^2\pmod{p^3}\end{aligned}$$

and

$$\begin{aligned}\sum_{x=1}^{p-1}\frac{1}{x^{p-1}}&\equiv pB_{\varphi(p^3)-(p-1)}\\&\equiv\binom{p^2-1}{2}pB_{2p-2}-(p^2-1)(p^2-3)pB_{p-1}+\binom{p^2-2}{2}(p-1)\\&\equiv\left(1-\frac{3p^2}{2}\right)pB_{2p-2}-(3-4p^2)pB_{p-1}+\left(3-\frac{5p^2}{2}\right)(p-1)\\&\equiv pB_{2p-2}-3pB_{p-1}+3(p-1)\pmod{p^3}.\end{aligned}$$

This concludes the proof. □

Remark 5.1. Let $p>5$ be a prime and $k\in\{1,2,\dots,p-5\}$. Using Corollary 4.1 and the method in the proof of Theorem 5.1 one can prove that

$$\sum_{x=1}^{p-1}\frac{1}{x^k}\equiv\begin{cases}-k\left(\frac{B_{3p-3-k}}{3p-3-k}-3\frac{B_{2p-2-k}}{2p-2-k}+3\frac{B_{p-1-k}}{p-1-k}\right)p-\binom{k+2}{3}\frac{p^3B_{p-3-k}}{p-3-k}\pmod{p^4} & \text{if } 2\mid k,\\ -\binom{k+1}{2}\left(\frac{B_{2p-3-k}}{2p-3-k}-2\frac{B_{p-2-k}}{p-2-k}\right)p^2\pmod{p^4} & \text{if } 2\nmid k.\end{cases}$$

From Theorem 5.1, Kummer's congruences and [17, Corollary 4.2] one can easily derive

Corollary 5.1. *Let p be a prime greater than 3 and $k \in \{1,2,\dots,p-1\}$. Then*

$$\sum_{x=1}^{p-1} \frac{1}{x^k} \equiv \begin{cases} \frac{k}{k+1} pB_{p-1-k} \pmod{p^2} & \text{if } k < p-1, \\ -pB_{p-1} + 2(p-1) \pmod{p^2} & \text{if } k = p-1. \end{cases}$$

Remark 5.2. In the cases $k = 1,3,\dots,p-4$ it follows from Corollary 5.1 that $\sum_{x=1}^{p-1}(1/x^k) \equiv 0 \pmod{p^2}$. This special result can be found in [10].

Theorem 5.2. *Let $p > 3$ be a prime.*
(a) *If $k \in \{2,4,\dots,p-5\}$, then*

$$\sum_{x=1}^{(p-1)/2} \frac{1}{x^k} \equiv \frac{k(2^{k+1}-1)}{2} \left(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k} \right) p \pmod{p^3}.$$

(b) *If $k \in \{3,5,\dots,p-4\}$, then*

$$\sum_{x=1}^{(p-1)/2} \frac{1}{x^k} \equiv (2^k-2) \left(2\frac{B_{p-k}}{p-k} - \frac{B_{2p-1-k}}{2p-1-k} \right) \pmod{p^2}.$$

(c) *If $q_p(2) = (2^{p-1}-1)/p$, then*

$$\sum_{x=1}^{(p-1)/2} \frac{1}{x} \equiv -2q_p(2) + pq_p^2(2) - \frac{2}{3}p^2 q_p^3(2) - \frac{7}{12}p^2 B_{p-3} \pmod{p^3}.$$

Proof. It is well known that [11]

$$\sum_{r=0}^{n-1} r^m = \frac{B_{m+1}(n) - B_{m+1}}{m+1},$$

$$B_m(x+y) = \sum_{r=0}^{m} \binom{m}{r} B_{m-r}(x) y^r$$

and

$$B_m(\tfrac{1}{2}) = (2^{1-m}-1)B_m.$$

Now suppose $k \in \{1,2,\dots,p-4\}$. Applying Euler's theorem we see that

$$\sum_{x=1}^{(p-1)/2} \frac{1}{x^k} \equiv \sum_{x=1}^{(p-1)/2} x^{\varphi(p^3)-k} = \frac{B_{\varphi(p^3)-k+1}\left(\frac{p+1}{2}\right) - B_{\varphi(p^3)-k+1}}{\varphi(p^3)-k+1}$$

$$= \frac{B_{\varphi(p^3)-k+1}\left(\frac{p+1}{2}\right) - B_{\varphi(p^3)-k+1}(\frac{1}{2})}{\varphi(p^3)-k+1} + \frac{B_{\varphi(p^3)-k+1}(\frac{1}{2}) - B_{\varphi(p^3)-k+1}}{\varphi(p^3)-k+1}$$

$$= \sum_{r=1}^{\varphi(p^3)-k+1} \frac{1}{r} \binom{\varphi(p^3)-k}{r-1} B_{\varphi(p^3)-k+1-r}\left(\frac{1}{2}\right) \left(\frac{p}{2}\right)^r$$

$$+\frac{B_{\varphi(p^3)-k+1}(\frac{1}{2})-B_{\varphi(p^3)-k+1}}{\varphi(p^3)-k+1}$$

$$\equiv \frac{p}{2}B_{\varphi(p^3)-k}\left(\frac{1}{2}\right)+\frac{p^2}{8}(\varphi(p^3)-k)B_{\varphi(p^3)-k-1}\left(\frac{1}{2}\right)$$

$$+\frac{2^{k-\varphi(p^3)}-2}{\varphi(p^3)-k+1}B_{\varphi(p^3)-k+1}$$

(observe that $p-1\nmid\varphi(p^3)-k-2$ and $p^{r-4}/r\in\mathbb{Z}_p$ for $r\geqslant 4$)

$$\equiv \frac{p}{2}(2^{k+1}-1)B_{\varphi(p^3)-k}-\frac{k}{8}p^2(2^{k+2}-1)B_{\varphi(p^3)-k-1}$$

$$+\frac{2^k-2^{\varphi(p^3)+1}}{\varphi(p^3)-k+1}B_{\varphi(p^3)-k+1} \pmod{p^3}.$$

If $k\in\{2,4,\ldots,p-5\}$, then $B_{\varphi(p^3)-k-1}=B_{\varphi(p^3)-k+1}=0$. By the above and (5.2) we get

$$\sum_{x=1}^{(p-1)/2}\frac{1}{x^k}\equiv\frac{2^{k+1}-1}{2}pB_{\varphi(p^3)-k}$$

$$\equiv\frac{2^{k+1}-1}{2}kp\left(\frac{B_{2p-2-k}}{2p-2-k}-2\frac{B_{p-1-k}}{p-1-k}\right) \pmod{p^3}.$$

This proves (a).

If $k\in\{3,5,\ldots,p-4\}$, then $B_{\varphi(p^3)-k-1}$, $B_{\varphi(p^3)-k+1}\in\mathbb{Z}_p$ and $B_{\varphi(p^3)-k}=0$. Thus, by the above and Corollary 4.1 (or (1.1)) we have

$$\sum_{x=1}^{(p-1)/2}\frac{1}{x^k}\equiv\frac{2^k-2}{\varphi(p^3)-k+1}B_{\varphi(p^3)-k+1}$$

$$\equiv(2^k-2)\left(-\frac{B_{2p-1-k}}{2p-1-k}+2\frac{B_{p-k}}{p-k}\right) \pmod{p^2}.$$

So (b) is true.

Now consider the case $k=1$. Since $pB_{\varphi(p^3)}\equiv p-1 \pmod{p^3}$ by [17, Corollary 4.1], we see that

$$\frac{2^{\varphi(p^3)}-1}{\varphi(p^3)}B_{\varphi(p^3)}=\frac{2^{\varphi(p^3)}-1}{p^3}\frac{pB_{\varphi(p^3)}}{p-1}\equiv\frac{(1+pq_p(2))^{p^2}-1}{p^3}$$

$$\equiv\frac{1}{p^3}\left\{\binom{p^2}{1}pq_p(2)+\binom{p^2}{2}p^2q_p^2(2)+\binom{p^2}{3}p^3q_p^3(2)\right\}$$

$$\equiv q_p(2)-\frac{1}{2}pq_p^2(2)+\frac{1}{3}p^2q_p^3(2) \pmod{p^3}.$$

Combining the above with (5.3) yields

$$\sum_{x=1}^{(p-1)/2}\frac{1}{x}\equiv-\frac{2^3-1}{8}\,p^2B_{\varphi(p^3)-2}-2\frac{2^{\varphi(p^3)}-1}{\varphi(p^3)}B_{\varphi(p^3)}$$

$$\equiv-\frac{7}{12}\,p^2B_{p-3}-2\left(q_p(2)-\frac{1}{2}pq_p^2(2)+\frac{1}{3}p^2q_p^3(2)\right)\pmod{p^3}.$$

This proves (c) and the proof is complete.

Remark 5.3. In 1938, Lehmer [13] proved that $\sum_{x=1}^{(p-1)/2}(1/x)\equiv-2q_p(2)+pq_p^2(2)\pmod{p^2}$ for any prime $p>3$. This result is now a consequence of Theorem 5.2(c).

Let $p>3$ be a prime and $k\in\{1,2,\ldots,p-4\}$. Observe that

$$1+\frac{1}{3^k}+\frac{1}{5^k}+\cdots+\frac{1}{(p-2)^k}=\sum_{x=1}^{p-1}\frac{1}{x^k}-\frac{1}{2^k}\sum_{x=1}^{(p-1)/2}\frac{1}{x^k}.$$

Using Theorems 5.1 and 5.2 one can establish similar results for $1+\frac{1}{3^k}+\frac{1}{5^k}+\cdots+\frac{1}{(p-2)^k}\pmod{p^3}$. For example,

$$1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{p-2}$$

$$\equiv q_p(2)-\frac{1}{2}pq_p^2(2)+\frac{1}{3}p^2q_p^3(2)-\frac{1}{24}p^2B_{p-3}\pmod{p^3}.$$

From Kummer's congruences and Theorem 5.2 we have

Corollary 5.2. *Let $p>5$ be a prime.*
(a) *If $k\in\{2,4,\ldots,p-5\}$, then*

$$\sum_{x=1}^{(p-1)/2}\frac{1}{x^k}\equiv\frac{k(2^{k+1}-1)}{2(k+1)}pB_{p-1-k}\pmod{p^2}.$$

(b) *If $k\in\{3,5,\ldots,p-4\}$, then*

$$\sum_{x=1}^{(p-1)/2}\frac{1}{x^k}\equiv-\frac{2^k-2}{k}B_{p-k}\pmod{p}.$$

6. A congruence for $(p-1)!\,(\mathrm{mod}\ p^3)$

Let p be a prime greater than 3. The classical Wilson's theorem states that $(p-1)!\equiv-1\pmod{p}$. In 1900 Glaisher [8] showed that $(p-1)!\equiv pB_{p-1}-p\pmod{p^2}$. Here we give a congruence for $(p-1)!$ modulo p^3.

Lemma 6.1 (Newton's formula [12]). *Suppose that* $x_1, x_2, \ldots, x_n$ *are complex numbers. If*

$$S_m = x_1^m + x_2^m + \cdots + x_n^m \quad \textit{and} \quad A_m = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_m},$$

then for $k = 0, 1, \ldots, n$ *we have*

$$S_k - A_1 S_{k-1} + A_2 S_{k-2} + \cdots + (-1)^{k-1} A_{k-1} S_1 + (-1)^k k A_k = 0.$$

Theorem 6.1. *For any prime* $p > 3$ *we have*

$$(p-1)! \equiv \frac{pB_{2p-2}}{2p-2} - \frac{pB_{p-1}}{p-1} - \frac{1}{2}\left(\frac{pB_{p-1}}{p-1}\right)^2 \pmod{p^3}.$$

Proof. For $k \in \{1, 2, \ldots, p-1\}$ set

$$S_k = 1^k + 2^k + \cdots + (p-1)^k, \quad A_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant p-1} i_1 \cdots i_k,$$

$$S_k^* = 1 + \frac{1}{2^k} + \cdots + \frac{1}{(p-1)^k} \quad \text{and} \quad A_k^* = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant p-1} \frac{1}{i_1 \cdots i_k}.$$

From Corollary 5.1 we know that

$$S_k^* \equiv \frac{k}{k+1} pB_{p-1-k} \pmod{p^2} \quad \text{for } k = 1, 2, \ldots, p-2.$$

Thus, by Newton's formula we have

$$A_k^* = \frac{(-1)^{k-1}}{k}\left(S_k^* + \sum_{r=1}^{k-1} (-1)^r A_r^* S_{k-r}^*\right) \equiv 0 \pmod{p} \quad (k = 1, 2, \ldots, p-2)$$

and so

$$A_k^* \equiv \frac{(-1)^{k-1}}{k} S_k^* \equiv \frac{(-1)^{k-1}}{k+1} pB_{p-1-k} \pmod{p^2} \quad (k = 1, 2, \ldots, p-1).$$

It then follows that

$$\begin{aligned}(-1)^r A_r^* S_{p-1-r}^* &\equiv -\frac{1}{r+1} pB_{p-1-r} \frac{p-1-r}{p-r} pB_r \\ &\equiv -\frac{B_r B_{p-1-r}}{r} p^2 \pmod{p^3} \quad (r = 1, 2, \ldots, p-2)\end{aligned}$$

and therefore that

$$\begin{aligned}A_{p-1}^* &= \frac{(-1)^{p-2}}{p-1}\left(S_{p-1}^* + \sum_{r=1}^{p-2} (-1)^r A_r^* S_{p-1-r}^*\right) \\ &\equiv -\frac{S_{p-1}^*}{p-1} - \left(\sum_{r=1}^{p-2} \frac{B_r B_{p-1-r}}{r}\right) p^2 \pmod{p^3}.\end{aligned}$$

Similarly, by (5.1), $S_k \equiv pB_k \pmod{p^2}$ for $k = 1, 2, \ldots, p-1$. Thus,

$$A_k = \frac{(-1)^{k-1}}{k}\left(S_k + \sum_{r=1}^{k-1}(-1)^r A_r S_{k-r}\right) \equiv 0 \pmod p \quad (k = 1, 2, \ldots, p-2)$$

and so

$$A_k \equiv \frac{(-1)^{k-1}}{k} S_k \equiv (-1)^{k-1}\frac{B_k}{k} p \pmod{p^2} \qquad (k = 1, 2, \ldots, p-1).$$

It then follows that

$$\begin{aligned} A_{p-1} &= -\frac{1}{p-1}\left(S_{p-1} + \sum_{r=1}^{p-2}(-1)^r A_r S_{p-1-r}\right) \\ &\equiv -\frac{S_{p-1}}{p-1} - \left(\sum_{r=1}^{p-2}\frac{B_r B_{p-1-r}}{r}\right) p^2 \pmod{p^3}. \end{aligned} \tag{6.1}$$

Notice that $A_{p-1}A^*_{p-1} = 1$. By the above we obtain

$$\frac{S^*_{p-1}S_{p-1}}{(p-1)^2} + \frac{S^*_{p-1} + S_{p-1}}{p-1}\left(\sum_{r=1}^{p-2}\frac{B_r B_{p-1-r}}{r}\right) p^2 \equiv 1 \pmod{p^3}. \tag{6.2}$$

It follows from Corollary 5.1, (5.1) and Theorem 5.1 that

$$S^*_{p-1} + S_{p-1} \equiv -pB_{p-1} + 2(p-1) + pB_{p-1} \equiv -2 \pmod p$$

and

$$\begin{aligned} S^*_{p-1}S_{p-1} &\equiv S^*_{p-1}(pB_{p-1} + 1 - 1) \\ &\equiv (-pB_{p-1} + 2(p-1))(pB_{p-1} + 1) \\ &\quad -(pB_{2p-2} - 3pB_{p-1} + 3(p-1)) \\ &= -pB_{2p-2} - (pB_{p-1})^2 + 2p^2B_{p-1} - (p-1) \pmod{p^3}. \end{aligned}$$

Hence, by (6.2) we get

$$\begin{aligned} &\left(\sum_{r=1}^{p-2}\frac{B_r B_{p-1-r}}{r}\right) p^2 \\ &\quad \equiv -\frac{p-1}{2} + \frac{-pB_{2p-2} - (pB_{p-1})^2 + 2p^2B_{p-1} - (p-1)}{2(p-1)} \pmod{p^3}. \end{aligned}$$

Putting this together with (6.1) yields

$$\begin{aligned} (p-1)! = A_{p-1} &\equiv -\frac{S_{p-1}}{p-1} - \left(\sum_{r=1}^{p-2}\frac{B_r B_{p-1-r}}{r}\right) p^2 \\ &\equiv -\frac{pB_{p-1}}{p-1} + \frac{p-1}{2} + \frac{pB_{2p-2} + (pB_{p-1})^2 - 2p^2B_{p-1} + (p-1)}{2(p-1)} \end{aligned}$$

(observe that $S_{p-1} \equiv pB_{p-1} \pmod{p^3}$ by (5.1))

$$= -\frac{pB_{p-1}}{p-1} + \frac{pB_{2p-2}}{2p-2} + \frac{-(pB_{p-1})^2 + p(pB_{p-1} - (p-1))^2}{2(p-1)^2}$$

$$\equiv -\frac{pB_{p-1}}{p-1} + \frac{pB_{2p-2}}{2p-2} - \frac{1}{2}\left(\frac{pB_{p-1}}{p-1}\right)^2 \pmod{p^3},$$

which completes the proof.

Remark 6.1. *The congruence* (6.1) *was first proved by Carlitz* [1].

7. Congruences concerning the least positive solution of $px \equiv r \,(\mathrm{mod}\, m)$

Suppose that $m, p \in \mathbb{Z}^+, r \in \mathbb{Z}$ and that p is prime to m. Throughout this section $A_r(m, p)$ denotes the least positive solution of the congruence $px \equiv r \,(\mathrm{mod}\, m)$.

Lemma 7.1. *Suppose that $m, p \in \mathbb{Z}^+$, $r \in \mathbb{Z}$, $0 < \langle r\rangle_{mp} < m + p$ and that p is prime to m. Then*

(a)

$$pA_r(m, p) + mA_r(p, m) = r + mp\left(1 - \left[\frac{r}{mp}\right]\right).$$

(b)

$$A_r(m, p) = m - \left[\frac{A_r(p, m)m}{p}\right] + \left[\frac{r}{p}\right] - m\left[\frac{r}{mp}\right].$$

Proof. Since p is prime to m, $pA_r(m, p) \equiv r \,(\mathrm{mod}\, m)$ and $mA_r(p, m) \equiv r \,(\mathrm{mod}\, p)$ we see that

$$pA_r(m, p) + mA_r(p, m) \equiv r \equiv \langle r\rangle_{mp} \pmod{mp}.$$

Clearly $A_r(p, m) \neq m$ or $A_r(p, m) \neq p$ since $\langle r\rangle_{mp} > 0$. So we have

$$\langle r\rangle_{mp} < p + m \leqslant pA_r(m, p) + mA_r(p, m) < pm + mp = 2mp.$$

Hence,

$$pA_r(m, p) + mA_r(p, m) = \langle r\rangle_{mp} + mp = r - mp\left[\frac{r}{mp}\right] + mp.$$

This proves (a).

Now consider (b). From (a) and the fact that $\langle mA_r(p, m)\rangle_p = \langle r\rangle_p = r - [r/p]p$ we obtain

$$A_r(m, p) = \frac{1}{p}\left(mp\left(1 - \left[\frac{r}{mp}\right]\right) + r - mA_r(p, m)\right)$$

$$= \frac{1}{p}\left(mp\left(1-\left[\frac{r}{mp}\right]\right)+r-\left(r-\left[\frac{r}{p}\right]p+p\left[\frac{A_r(p,m)m}{p}\right]\right)\right)$$

$$= m-\left[\frac{A_r(p,m)m}{p}\right]+\left[\frac{r}{p}\right]-m\left[\frac{r}{mp}\right].$$

This completes the proof. □

Theorem 7.1. *Let p be an odd prime, $m,n \in \mathbb{Z}^+$, $r \in \mathbb{Z}$, $p \nmid m$ and $0 < \langle r\rangle_{mp} < m+p$. Then*
(a)

$$A_r(m,p) \equiv r-m\left[\frac{r}{mp}\right]-mB_{\varphi(p^{n+1})+1}\left(\frac{r}{m}\right)$$

$$\equiv r-m\left[\frac{r}{mp}\right]-m\frac{B_{\varphi(p^n)+1}(\frac{r}{m})}{\varphi(p^n)+1} \pmod{p^n}.$$

(b) *If $p>n$ then*

$$A_r(m,p) \equiv r-m\left[\frac{r}{mp}\right]+m\sum_{k=1}^{n}\binom{n}{k}(-1)^k\frac{B_{k(p-1)+1}(\frac{r}{m})}{k(p-1)+1} \pmod{p^n}.$$

Proof. It is clear that

$$\left\langle -\frac{r}{m}\right\rangle_p = p-A_r(p,m).$$

From this and Lemma 7.1(a) we get

$$\frac{\frac{r}{m}+\langle -\frac{r}{m}\rangle_p}{p} = \frac{\frac{r}{m}+p-A_r(p,m)}{p} = \frac{r+mp-mA_r(p,m)}{mp}$$

$$= \frac{pA_r(m,p)+mp[\frac{r}{mp}]}{mp} = \frac{A_r(m,p)}{m}+[\tfrac{r}{mp}].$$

Combining this with [17, Corollary 4.1] we find

$$pB_{\varphi(p^{n+1})+1}\left(\frac{r}{m}\right) \equiv p\left(B_1\left(\frac{r}{m}\right)-B_1\left(\frac{A_r(m,p)}{m}+\left[\frac{r}{mp}\right]\right)\right) \pmod{p^{n+1}}.$$

Since $B_1(x)=x-\frac{1}{2}$ we have

$$B_{\varphi(p^{n+1})+1}\left(\frac{r}{m}\right) \equiv \frac{r-A_r(m,p)}{m}-\left[\frac{r}{mp}\right] \pmod{p^n}.$$

Also, using Corollary 3.1 we obtain

$$\frac{B_{\varphi(p^n)+1}(\frac{r}{m})}{\varphi(p^n)+1} \equiv B_1\left(\frac{r}{m}\right)-B_1\left(\frac{A_r(m,p)}{m}+\left[\frac{r}{mp}\right]\right)$$

$$= \frac{r-A_r(m,p)}{m}-\left[\frac{r}{mp}\right] \pmod{p^n}.$$

This proves part (a).

As for part (b), we notice that $p-1\geqslant n$ and so that

$$\frac{r-A_r(m,p)}{m}-\left[\frac{r}{mp}\right]+\sum_{k=1}^{n}\binom{n}{k}(-1)^k\frac{B_{k(p-1)+1}(\frac{r}{m})}{k(p-1)+1}$$

$$\equiv\sum_{k=0}^{n}\binom{n}{k}(-1)^k\frac{B_{k(p-1)+1}\left(\frac{r}{m}\right)-p^{k(p-1)}B_{k(p-1)+1}\left(\frac{A_r(m,p)}{m}+\left[\frac{r}{mp}\right]\right)}{k(p-1)+1}$$

$$\equiv 0 \pmod{p^n} \quad \text{(by Theorem 3.2).}$$

Theorem 7.2. *Let p be an odd prime, $m\in\mathbb{Z}^+$, $r\in\mathbb{Z}$, $0<\langle r\rangle_{mp}<m+p$ and $p\nmid m$.*
(a) *If $p\nmid r$, then*

$$A_r(m,p)\equiv -m\left[\frac{r}{mp}\right]+\frac{m}{2}-r\frac{pB_{p-1}-(p-1)}{p}+\frac{rm^{p-1}-r^p}{p}$$
$$+\sum_{k=1}^{(p-3)/2}\frac{m^{2k}}{r^{2k-1}}\frac{B_{2k}}{2k} \pmod p.$$

(b)

$$A_r(m,p)\equiv -m\left[\frac{r}{mp}\right]+r-\frac{m}{2}-\frac{1}{p^2}\sum_{k=0}^{p-1}(km+r)^p \pmod p.$$

Proof. From Theorem 7.1 and the congruence $\binom{p-1}{s}\equiv(-1)^s \pmod p$ we see that

$$A_r(m,p)+m\left[\frac{r}{mp}\right]$$

$$\equiv r-m\frac{B_p\left(\frac{r}{m}\right)}{p}=r-\frac{m}{p}\sum_{k=0}^{p}\binom{p}{k}B_k\left(\frac{r}{m}\right)^{p-k}$$

$$=r-\frac{m}{p}\left(\left(\frac{r}{m}\right)^p+pB_1\left(\frac{r}{m}\right)^{p-1}+pB_{p-1}\frac{r}{m}\right.$$

$$\left.+\sum_{k=1}^{(p-3)/2}\frac{p}{2k}\binom{p-1}{2k-1}B_{2k}\left(\frac{r}{m}\right)^{p-2k}\right)$$

$$\equiv\frac{m}{2}-r\frac{pB_{p-1}-(p-1)}{p}+\frac{rm^{p-1}-r^p}{p}+\sum_{k=1}^{(p-3)/2}\frac{B_{2k}}{2k}\frac{m^{2k}}{r^{2k-1}} \pmod p.$$

This proves part (a).

Now consider part (b). It follows from [17, Lemma 2.3] that $pB_k(x), B_k(x)-B_k \in \mathbb{Z}_p$ for $x \in \mathbb{Z}_p$. Also, $B_k(x+1)=B_k(x)+kx^{k-1}$ and $B_k(x+y)=\sum_{s=0}^{k}\binom{k}{s}B_{k-s}(x)y^s$. Hence,

$$\begin{aligned}\sum_{a=0}^{p-1}(a+x)^p &= \sum_{a=0}^{p-1}\frac{B_{p+1}(a+x+1)-B_{p+1}(a+x)}{p+1} = \frac{B_{p+1}(p+x)-B_{p+1}(x)}{p+1}\\ &= \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}(x)p^k\\ &\equiv \frac{1}{p+1}\left((p+1)pB_p(x)+\frac{(p+1)p}{2}p^2B_{p-1}(x)\right)\\ &= pB_p(x)+\frac{p^3}{2}(B_{p-1}(x)-B_{p-1}+B_{p-1})\\ &\equiv pB_p(x)+\frac{p^2}{2}\,pB_{p-1} \equiv pB_p(x)-\frac{p^2}{2} \pmod{p^3}.\end{aligned}$$

That is,

$$\frac{B_p(x)}{p} \equiv \frac{1}{2}+\frac{1}{p^2}\sum_{a=0}^{p-1}(a+x)^p \pmod{p}. \tag{7.1}$$

Putting this together with Theorem 7.1 yields

$$\begin{aligned}A_r(m,p)+m\left[\frac{r}{mp}\right] &\equiv r-m\frac{B_p(\frac{r}{m})}{p} \equiv r-m\left(\frac{1}{2}+\frac{1}{p^2}\sum_{k=0}^{p-1}\left(k+\frac{r}{m}\right)^p\right)\\ &\equiv r-\frac{m}{2}-\frac{1}{p^2}\sum_{k=0}^{p-1}(km+r)^p \pmod{p}.\end{aligned}$$

The proof is now complete.

Remark 7.1. *In the cases* $r=1,2,\ldots,p-1$ *Theorem* 7.2(a) *was proved by Vandiver* [19].

Theorem 7.3. *Let* p *be an odd prime.*
(a) *If* $r \in \{1,2,\ldots,p-1\}$, *then*

$$\frac{r^{p-1}-1}{p} \equiv -2\,\frac{pB_{p-1}-(p-1)}{p}+\frac{1}{r}\sum_{m=1}^{p-1}A_r(m,p) \pmod{p}.$$

(b) *If* $m \in \mathbb{Z}^+$ *and* $p \nmid m$, *then*

$$\frac{m^{p-1}-1}{p} \equiv -\sum_{r=1}^{p-1}\frac{A_r(m,p)}{r} \pmod{p}.$$

(c) *For* $m \in \mathbb{Z}^+$ *we have*

$$\frac{m^p - m}{p} \equiv \sum_{k=1}^{p-1} \frac{1}{k}\left[\frac{km}{p}\right] \pmod p.$$

Proof. Suppose $r \in \{1, 2, \ldots, p-1\}$. It follows from (5.1) that

$$\sum_{m=1}^{p-1} m \equiv 0 \pmod p, \quad \sum_{m=1}^{p-1} m^{p-1} \equiv pB_{p-1} \pmod{p^2}$$

and

$$\sum_{m=1}^{p-1} m^{2k} \equiv 0 \pmod p \quad \text{for } k = 1, 2, \ldots, \frac{p-3}{2}.$$

Thus, by Theorem 7.2(a) we get

$$\begin{aligned}\sum_{m=1}^{p-1} A_r(m,p) &\equiv -(p-1)r\frac{pB_{p-1}-(p-1)}{p} + \frac{rpB_{p-1}-(p-1)r^p}{p}\\ &= (2-p)r\frac{pB_{p-1}-(p-1)}{p} + \frac{-r^p+r}{p}(p-1)\\ &\equiv 2r\frac{pB_{p-1}-(p-1)}{p} + \frac{r^p-r}{p} \pmod p.\end{aligned}$$

This proves (a).

Let us consider (b). Observe that $\sum_{r=1}^{p-1} r^{p-1} \equiv pB_{p-1} \pmod{p^2}$ by (5.1). Applying Theorem 7.2(a) we see that

$$\begin{aligned}\sum_{r=1}^{p-1} \frac{A_r(m,p)}{r} &\equiv \frac{m}{2}\sum_{r=1}^{p-1}\frac{1}{r} - (p-1)\frac{pB_{p-1}-(p-1)}{p}\\ &\quad + \frac{(p-1)m^{p-1} - \sum_{r=1}^{p-1} r^{p-1}}{p} + \sum_{k=1}^{(p-3)/2} \frac{m^{2k}B_{2k}}{2k}\sum_{r=1}^{p-1}\frac{1}{r^{2k}}\\ &\equiv \frac{pB_{p-1}-(p-1)}{p} + \frac{(p-1)m^{p-1} - pB_{p-1}}{p}\\ &\equiv -\frac{m^{p-1}-1}{p} \pmod p.\end{aligned}$$

So (b) is true.

Now consider (c). If $m = np$ for some $n \in \mathbb{Z}$, then

$$\sum_{k=1}^{p-1} \frac{1}{k}\left[\frac{km}{p}\right] = \sum_{k=1}^{p-1} \frac{1}{k} \cdot kn \equiv -n \equiv \frac{m^p - m}{p} \pmod p.$$

So (c) is true when $p|m$.

If $p \nmid m$, by using (b) and Lemma 7.1(b) we obtain

$$\begin{aligned}\frac{m^p-m}{p} &\equiv -m\sum_{r=1}^{p-1}\frac{A_r(m,p)}{r} = -\sum_{r=1}^{p-1}\frac{m}{r}\left(m-\left[\frac{mA_r(p,m)}{p}\right]\right)\\ &\equiv \sum_{r=1}^{p-1}\frac{m}{r}\left[\frac{mA_r(p,m)}{p}\right] \equiv \sum_{r=1}^{p-1}\frac{1}{A_r(p,m)}\left[\frac{mA_r(p,m)}{p}\right]\\ &\equiv \sum_{k=1}^{p-1}\frac{1}{k}\left[\frac{km}{p}\right] \pmod p\end{aligned}$$

(observe that $\{A_1(p,m),\dots,A_{p-1}(p,m)\} = \{1,\dots,p-1\}$).

This completes the proof.

Remark 7.2. Theorem 7.3(b) was first obtained by my brother Zhi-Wei Sun. In fact, he proved that

$$\frac{m^{p-1}-1}{p} \equiv -\sum_{x=1}^{m} x \sum_{\substack{r=1\\ r\equiv px \pmod m}}^{p-1} \frac{1}{r} \pmod p,$$

where p is an odd prime and $p \nmid m$. We mention that the paper of Dilcher and Skula [4] comes close to it. Theorem 7.3(c) was found by Lerch and Baker [3] in 1906, and it can also be deduced from the following interesting identity:

$$\sum_{r=0}^{n}\binom{n}{r}(-1)^{n-r}\binom{rm}{n} = m^n.$$

Corollary 7.1. *Let p be an odd prime. Then*

$$\frac{(p-1)!+1}{p} \equiv \frac{1}{2}\sum_{m=1}^{p-1} x_m \pmod p,$$

where $x_m \in \{1,2,\dots,m\}$ *and* $px_m \equiv 1 \pmod m$.

Proof. Taking $r=1$ in Theorem 7.3(a) we find

$$\sum_{m=1}^{p-1} x_m \equiv 2\frac{pB_{p-1}-(p-1)}{p} \pmod p.$$

Putting this together with the known fact that $(p-1)! \equiv pB_{p-1} - p \pmod{p^2}$ gives the result.

To end this section, we point out the following related results:

Suppose that $k, m, p-1 \in \mathbb{Z}^+$, $n \in \mathbb{Z}$, or $\{n/m\} = n/m - [n/m]$ and that p is prime to m. Then

$$\sum_{r=0}^{p-1} A_{r-n}(m,p) r^{k-1} \equiv \frac{B_k - m^k B_k(\{\frac{n}{m}\})}{k} + (m+1)\left(1 - \frac{m^{k-1}}{2}\right) pB_{k-1} + (m+1)\left(1 - \frac{m^{k-2}}{2}\right)\frac{k-1}{2} p^2 B_{k-2} \pmod p. \tag{7.2}$$

The generalization of Voronoi congruences: Let $k, m, p-1 \in \mathbb{Z}^+$ and $n \in \mathbb{Z}$. If p is prime to m, then

$$\frac{m^k B_k(\frac{n}{m}) - B_k}{k} \equiv \sum_{j=0}^{p-1} (jm+n)^{k-1}\left[\frac{jm+n}{p}\right] + \left(1 - \frac{(m+1)m^{k-1}}{2}\right) pB_{k-1} + \left(1 - \frac{(m+1)m^{k-2}}{2}\right)\frac{k-1}{2} p^2 B_{k-2} \pmod p. \tag{7.3}$$

These results will be proved in another paper.

8. Congruences for generalized Bernoulli numbers

Let χ be a Dirichlet character modulo positive integer m. The generalized Bernoulli number $B_{n,\chi}$ is defined by

$$\sum_{r=1}^{m} \frac{\chi(r) t e^{rt}}{e^{mt}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

It is well known that [20]

$$B_{1,\chi_0} = \frac{1}{2}, \quad B_{n,\chi_0} = B_n \ (n \neq 1) \qquad \text{and} \qquad B_{n,\chi} = m^{n-1} \sum_{r=1}^{m} \chi(r) B_n\left(\frac{r}{m}\right),$$

where χ_0 is the trivial character.

Inspired by Sections 3 and 4, we now establish similar results for generalized Bernoulli numbers.

Lemma 8.1. *Let χ be a Dirichlet character modulo m, and p a prime such that $p \nmid m$.* (a) *If $n, b \in \mathbb{Z}^+$ and $p-1 \nmid b$, then*

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k (1 - \chi(p) p^{k(p-1)+b-1}) \frac{B_{k(p-1)+b,\chi}}{k(p-1)+b} \equiv 0 \pmod{p^n}.$$

(b) *If $\chi \neq \chi_0$, $n \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+ \cup \{0\}$, then*

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k (1 - \chi(p) p^{k(p-1)+b-1}) pB_{k(p-1)+b,\chi} \equiv 0 \pmod{p^n}.$$

Proof. For $r=1,2,\ldots,m$ denote the least positive solution of the congruence $px\equiv r\,(\mathrm{mod}\,m)$ by $A_r(m,p)$. It is easily seen that

$$\left\langle -\frac{r}{m}\right\rangle_p=\frac{pA_r(m,p)-r}{m}\quad\text{and}\quad \{A_1(m,p),\ldots,A_m(m,p)\}=\{1,2,\ldots,m\}.$$

Since

$$B_{k(p-1)+b,\chi}=m^{k(p-1)+b-1}\sum_{r=1}^{m}\chi(r)B_{k(p-1)+b}\left(\frac{r}{m}\right),$$

we have

$$\begin{aligned}\chi(p)p^{k(p-1)+b-1}&B_{k(p-1)+b,\chi}\\ &=\chi(p)p^{k(p-1)+b-1}\cdot m^{k(p-1)+b-1}\sum_{s=1}^{m}\chi(s)B_{k(p-1)+b}\left(\frac{s}{m}\right)\\ &=(mp)^{k(p-1)+b-1}\sum_{s=1}^{m}\chi(ps)B_{k(p-1)+b}\left(\frac{s}{m}\right)\\ &=(mp)^{k(p-1)+b-1}\sum_{r=1}^{m}\chi(pA_r(m,p))B_{k(p-1)+b}\left(\frac{A_r(m,p)}{m}\right)\\ &=(mp)^{k(p-1)+b-1}\sum_{r=1}^{m}\chi(r)B_{k(p-1)+b}\left(\frac{A_r(m,p)}{m}\right)\end{aligned}$$

and therefore

$$\begin{aligned}(1-\chi(p)p^{k(p-1)+b-1})&B_{k(p-1)+b,\chi}\\ &=\sum_{r=1}^{m}\chi(r)m^{k(p-1)+b-1}\left(B_{k(p-1)+b}\left(\frac{r}{m}\right)-p^{k(p-1)+b-1}B_{k(p-1)+b}\left(\frac{A_r(m,p)}{m}\right)\right).\end{aligned}\tag{8.1}$$

Suppose $b\not\equiv 0\,(\mathrm{mod}\,p-1)$. From Fermat's little theorem and Theorem 3.2 we know that both $m^{k(p-1)+b-1}$ and $(B_{k(p-1)+b}(r/m)-p^{k(p-1)+b-1}B_{k(p-1)+b}(A_r(m,p)/m))/(k(p-1)+b)$ are p-regular functions. Putting this together with Theorem 2.3 yields

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}(-1)^k m^{k(p-1)+b-1}&\frac{B_{k(p-1)+b}(\frac{r}{m})-p^{k(p-1)+b-1}B_{k(p-1)+b}(\frac{A_r(m,p)}{m})}{k(p-1)+b}\\ &\equiv 0 \pmod{p^n}.\end{aligned}$$

Hence, by (8.1) we get

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k(1-\chi(p)p^{k(p-1)+b-1})\frac{B_{k(p-1)+b,\chi}}{k(p-1)+b}\equiv 0 \pmod{p^n}.$$

This proves part (a).

Now consider part (b). From the proof of Lemma 2.1 we see that

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k m^{k(p-1)+b-1}\left(pB_{k(p-1)+b}\left(\frac{r}{m}\right)-p^{k(p-1)+b}B_{k(p-1)+b}\right.$$

$$\left.\left(\frac{A_r(m,p)}{m}\right)\right)=\sum_{s=0}^{n}\binom{n}{s}\left(\sum_{t=0}^{n-s}\binom{n-s}{t}(-1)^t m^{(s+t)(p-1)+b-1}\right)$$

$$\left(\sum_{t=0}^{s}\binom{s}{t}(-1)^t\left(pB_{t(p-1)+b}\left(\frac{r}{m}\right)-p^{t(p-1)+b}B_{t(p-1)+b}\left(\frac{A_r(m,p)}{m}\right)\right)\right).$$

Since

$$\sum_{t=0}^{n-s}\binom{n-s}{t}(-1)^t m^{(s+t)(p-1)+b-1}=m^{s(p-1)+b-1}(1-m^{p-1})^{n-s}\equiv 0 \pmod{p^{n-s}}$$

and

$$\sum_{t=0}^{s}\binom{s}{t}(-1)^t\left(pB_{t(p-1)+b}\left(\frac{r}{m}\right)-p^{t(p-1)+b}B_{t(p-1)+b}\left(\frac{A_r(m,p)}{m}\right)\right)$$

$$\equiv p^{s-1}\delta(s,b,p)\equiv\begin{cases}p^{s-1}\pmod{p^s} & \text{if } B_s\notin\mathbb{Z}_p \text{ and } p-1\mid b,\\ 0\pmod{p^s} & \text{if } B_s\in\mathbb{Z}_p \text{ or } p-1\nmid b\end{cases}$$

by [17, Theorem 3.1], in view of (8.1) and the above we obtain

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k(1-\chi(p)p^{k(p-1)+b-1})pB_{k(p-1)+b,\chi}$$

$$=\sum_{r=1}^{m}\chi(r)\sum_{k=0}^{n}\binom{n}{k}(-1)^k m^{k(p-1)+b-1}$$

$$\left(pB_{k(p-1)+b}\left(\frac{r}{m}\right)-p^{k(p-1)+b}B_{k(p-1)+b}\left(\frac{A_r(m,p)}{m}\right)\right)$$

$$\equiv\sum_{r=1}^{m}\chi(r)p^{n-1}\sum_{s=0}^{n}\binom{n}{s}m^{s(p-1)+b-1}\left(\frac{1-m^{p-1}}{p}\right)^{n-s}\delta(s,b,p)$$

$$=0 \pmod{p^n},$$

which completes the proof.

We are now able to give

Theorem 8.1. *Let χ be a Dirichlet character modulo m, and p a prime for which $p\nmid m$.*

(a) *If* $n, b \in \mathbb{Z}^+$ *and* $p-1 \nmid b$, *then*

$$(1-\chi(p)p^{k(p-1)+b-1})\frac{B_{k(p-1)+b,\chi}}{k(p-1)+b}$$

$$\equiv \sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r}(1-\chi(p)p^{r(p-1)+b-1})\frac{B_{r(p-1)+b,\chi}}{r(p-1)+b}$$

$$\equiv a_{n-1}k^{n-1}+\cdots+a_1k+a_0 \pmod{p^n}$$

for every $k=0,1,2,\ldots,$ *where* $a_0,\ldots,a_{n-1}$ *are all integers.*

(b) *If* $n \in \mathbb{Z}^+$, $b \in \mathbb{Z}^+ \cup \{0\}$ *and* $\chi \neq \chi_0$, *then*

$$(1-\chi(p)p^{k(p-1)+b-1})pB_{k(p-1)+b,\chi}$$

$$\equiv \sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r}(1-\chi(p)p^{r(p-1)+b-1})pB_{r(p-1)+b,\chi}$$

$$\equiv a_{n-1}k^{n-1}+\cdots+a_1k+a_0 \pmod{p^n}$$

for every $k=0,1,2,\ldots,$ *where* $a_0,\ldots,a_{n-1}$ *are all integers.*

Proof. This is immediate from Lemma 8.1, Theorems 2.1 and 2.2.

9. Uncited References

The following references are also of importance to the reader: [1,3,5,6,9,14,16]

References

[1] L. Carlitz, A theorem of Glaisher, Can. J. Math. 5 (1953) 306–316.
[2] L. Comtet, Advanced Combinatorics (The Art of Finite and Infinite Expansions), D. Reidel Publishing Company, Dordrecht, 1974. (Trans. J.W. Nienhuys).
[3] L.E. Dickson, History of the Theory of Numbers, Vol. I, Chelsea, New York, 1952.
[4] K. Dilcher, L. Skula, A new criterion for the first case of Fermat's last theorem, Math. Comput. 64 (1995) 363–392.
[5] K. Dilcher, L. Skula, I.Sh. Slavutskiĭ, Bernoulli Numbers Bibliography (1713–1990), Queen's Papers in Pure and Applied Mathematics, No. 87, Kingston, Ontario, 1991.
[6] R. Ernnvall, Generalized Bernoulli numbers, generalized irregular primes, and class number, Ann. Univ. Turku. Ser. A 1 (1979) 1–72; MR 80m:12002.
[7] F.S. Gilllespie, A generalization of Kummer's congruences and related results, Fibonacci Quart. 30 (1992) 349–367.
[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, Quarterly J. Math. 31 (1900) 321–353.
[9] A. Granville, Z.W. Sun, Values of Bernoulli polynomials, Pacific J. Math. 172 (1996) 117-137.
[10] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, 5th Edition, Oxford Univ. Press, Oxford, 1981, p. 104.
[11] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer, New York, 1982, pp. 239–248.

[12] N. Jacobson, Basic Algebra I, 2nd Edition, W.H. Freeman Publishing Company, New York, 1985, p. 140.
[13] E. Lehmer, On congruences involving Bernoulli numbers and quotients of Fermat and Wilson, Ann. Math. 39 (1938) 350–360.
[14] N. Nielson, Traité Élémentaire des Nombres Bernoulli, Paris, 1923.
[15] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer, New York, 1979, p. 158.
[16] H.R. Stevens, Bernoulli numbers and Kummer's criterion, Fibonacci Quart. 24 (1986) 154–159.
[17] Z.H. Sun, Congruences for Bernoulli numbers and Bernoulli polynomials, Discrete Math. 163 (1997) 153–163.
[18] I. Tomescu, Problems in Combinatorics and Graph Theory, Wiley, New York, 1985, p. 9 (Trans. R.A. Melter).
[19] H.S. Vandiver, Certain congruences involving the Bernoulli numbers, Duke Math. J. 5 (1939) 548–551.
[20] L.C. Washington, Introduction to Cyclotomic Fields, Springer, New York, 1982, pp. 30–31, 61–62,64,141.