EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 1, No. 4, 2008, (3-21)
ISSN 1307-5543 – www.ejpam.com

Voronoï type congruences and its applications

Takashi Agoh[*,†]

Department of Mathematics, Tokyo University of Science, Noda, Chiba 278-8510, Japan

Abstract. In this paper, we will first deduce Voronoï type congruences for Bernoulli numbers in the even suffix notation. Continuously, we will apply them to extend very important arithmetic properties (such as von Staudt-Clausen's and Kummer's congruences) of these numbers to more general situation.

AMS subject classifications: 11A07, 11B68, 11Y1

Key words: Bernoulli numbers, Von Staudt-Clausen's theorem, Voronoï's congruence, Kummer's congruence, Irregular primes

1. Introduction

The Bernoulli numbers B_m $(m \geq 0)$ are defined by the Taylor expansion

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} \frac{B_m}{m!} t^m, \quad |t| < 2\pi.$$

These numbers may be also defined by the recurrence relation

$$B_m = -\frac{1}{m+1} \sum_{i=0}^{m-1} \binom{m+1}{i} B_i, \; B_0 = 1.$$

It is easily seen that $B_{2m+1} = 0$ and $(-1)^{m-1} B_{2m} > 0$ for all $m \geq 1$. Using the Stirling formula $n! \sim (n/e)^n \sqrt{2\pi n}$, we see asymptotically $|B_{2m}| \sim 4\sqrt{\pi m}(m/\pi e)^{2m}$. Further, if $3 \leq m < n$, then $|B_{2m}/2m| < |B_{2n}/2n|$, and also $|B_{2m}|/(2m)^{\lambda} \to \infty$ as $m \to \infty$ for every $\lambda \geq 1$.

Let $m \geq 2$ be even and $n \geq 1$. If we write $B_m = N_m/D_m$ $(N_m, D_m \in \mathbb{Z},\, D_m > 0)$ in lowest terms, then the Voronoï congruence can be stated as

$$(a^m - 1) N_m \equiv m D_m \sum_{j=1}^{n-1} (aj)^{m-1} \left[\frac{aj}{n} \right] \pmod{n}, \tag{1.1}$$

[*] *Email address:* `agoh_takashi@ma.noda.sut.ac.jp` (T. Agoh)

[†] The author was supported in part by a grant of the Ministry of Education, Science and Culture of Japan.

where a is a positive integer with $(a,n)=1$ and $[aj/n]$ is the greatest integer $\leq aj/n$. Applying the Voronoï and his type congruences, we are able to deduce various arithmetical properties of Bernoulli numbers. For surrounding landscape on these congruences, see Porubský's expository article [14].

The prime factorization of D_m can be explicitly stated by the von Staudt-Clausen theorem which asserts that $p-1 \mid m$ if and only if $p \mid D_m$ for a prime p. Further, we know that D_m is square-free. In contrast with the denominator, much less is known about prime divisors of N_m. One of conspicuous facts is von Staudt's theorem (although this is commonly called Adams' theorem) which mentions that, for an odd prime p and an even integer $m \geq 2$, if $p-1 \nmid m$ and $p^e \mid m$ $(e \geq 1)$, then $p^e \mid N_m$. If we take account of this result, then the question how to find prime divisors of the numerator of B_m/m necessarily arises.

The famous congruence $B_m/m \equiv B_l/l \pmod{p}$ (p a prime ≥ 5) for even integers $m,l \geq 2$ such that $m \equiv l \pmod{p-1}$ and $p-1 \nmid m$ is due to von Staudt and Kummer, and it shows that B_m/m has period $p-1$. We can further state that if $p-1 \nmid m$ and $m \equiv l \pmod{\varphi(p^s)}$ $(s \geq 1,\ \varphi$ the Euler totient function), then

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{l-1})\frac{B_l}{l} \pmod{p^s}. \tag{1.2}$$

This congruence is nothing but a special case of more general formulas given in Theorem 4.1 below, however it is needless to say that this deeply concerns with the construction of p-adic L function. One can consult more details with the beautiful books by Iwasawa [9] and Washington [17].

An odd prime p is said to be *irregular* if p divides the class number h_p of the cyclotomic field $\mathbb{Q}(\zeta_p)$ defined by ζ_p a primitive pth root of unity. Otherwise, it is said to be *regular*. These notions were first brought by Kummer in his work on Fermat's Last Theorem. As an irregularity criterion, Kummer showed that p is irregular if and only if p divides at least one of numerators of the $(p-3)/2$ Bernoulli numbers $B_2, B_4, ..., B_{p-3}$. It therefore requires to obtain appropriate congruences for getting residues modulo p of B_{2k} $(1 \leq k \leq (p-3)/2)$.

Amazingly, Jensen [10] proved in 1915 that there are infinitely many irregular primes of the form $p \equiv 3 \pmod{4}$. The proof was rather easy and, in fact, only some basic arithmetic properties of Bernoulli numbers were used. However, in spite of various efforts by many mathematicians, it has not yet been shown whether there are infinitely many regular primes. Here we should note that Siegel (1964) proved that, under heuristic assumptions, the density of regular primes among the set of all primes is $1/\sqrt{e} \approx 0.6065$.

In this paper, we will first deduce various Voronoï type congruences by generalizing his original (1.1). Applying these, we will extend important arithmetic properties (including von Studt-Clausen's congruence) on Bernoulli numbers to more general situation. Further we will discuss specific properties of the numerator of B_m/m, whose prime divisors are all irregular.

2. General discussion on Bernoulli numbers

In this section, we shall introduce fundamental theorems which are narrating to us very important arithmetical properties of Bernoulli numbers.

In what follows, we write B_m and $\beta_m = B_m/m$ ($m \geq 2$ is even) in lowest terms as follows:

$$B_m = \frac{N_m}{D_m} \quad \text{and} \quad \beta_m = \frac{N'_m}{D'_m},$$

where $(N_m, D_m) = (N'_m, D'_m) = 1$ and $D_m, D'_m > 0$.

Concerning divisibility properties of the numerator N_m of B_m, we have the following result which is widely known as *Adams' theorem*. However, it would be better to call *von Staudt's theorem* according to Slavutskii's suggestion written in his historical observation [15] on von Staudt's achievements, because this result was first attributed to von Staudt in 1845 before Adams (1878).

Theorem 2.1. *Let $m \geq 2$ be an even integer. If $m = p^e m_0$ ($e \geq 1$, p an odd prime, $p \nmid m_0$) and $p \nmid D_m$, then $p^e \mid N_m$.*

We see from this theorem that $p \nmid D_m$ if and only if $p \nmid D'_m$. The divisor p^e of N_m stated above is called an *improper divisor* of B_m. If $d > 0$ divides N_m but not m, then it is called a *proper divisor* of B_m. We can easily show that p is irregular if and only if p is a proper divisor of some Bernoulli number. It is unknown whether there exists an odd prime p such that $B_m \equiv 0 \pmod{p^2}$ for an even m, $2 \leq m \leq p-3$.

The next theorem is known as the *Euler-MacLaurin summation formula*. The proof can be easily performed by equating the coefficients of t^{m+1} in the power series expansions of both sides of the identity

$$t\sum_{i=0}^{n-1} e^{it} = \frac{t}{e^t - 1}(e^{nt} - 1).$$

Theorem 2.2. *Let $m, n \geq 1$ and $S_m(n) = 1^m + 2^m + \cdots + (n-1)^m$. Then*

$$S_m(n) = \sum_{j=1}^{m+1} \frac{1}{j}\binom{m}{j-1} B_{m+1-j} n^j.$$

Suppose that $p^\alpha \parallel 2i+1$ for $p \geq 5$ and $i \geq 2$. Thus, we can write as $2i+1 = p^\alpha x$ ($\alpha \geq 1$, $p \nmid x$). Since $p^\alpha x - \alpha \geq 5^\alpha - \alpha \geq 4$,

$$\frac{1}{2i+1} p^{2i+1} = \frac{1}{x} p^{p^\alpha x - \alpha} \equiv 0 \pmod{p^4}.$$

Also, since $\mathrm{ord}_3(D_m) = 1$ for all even $m \geq 2$, we know $\left(3^2 B_{m-2}\right) D_m \equiv 0 \pmod{3^2}$, which implies from Theorem 2.2 the following

Theorem 2.3. *If $m \geq 2$ is even and $n \geq 1$, then*

$$D_m S_m(n) \equiv N_m n \pmod{n^2}.$$

We now introduce the Voronoï congruence which brings various important properties of Bernoulli numbers in relief. Let a and n be positive integers prime to each other. Suppose that q_j and r_j, $j = 1,2,...,n-1$, are positive integers satisfying $aj = q_jn + r_j$, $0 < r_j < n$. Here $q_j = [aj/n]$. By direct calculation of $(aj - q_jn)^m = r_j^m$ we obtain

$$(aj)^m - r_j^m = \sum_{i=1}^{m}(-1)^{i-1}\binom{m}{i}(aj)^{m-i}n^i\left[\frac{aj}{n}\right]^i.$$

Noting that $\{r_j \mid j = 1,2,...,n-1\} = \{1,2,...,n-1\}$, if we sum over $j = 1,2,...,n-1$, then

$$(a^m - 1)S_m(n) = \sum_{i=1}^{m}(-1)^{i-1}n^i\binom{m}{i}\sum_{j=1}^{n}(aj)^{m-i}\left[\frac{aj}{n}\right]^i, \tag{2.1}$$

so that

$$(a^m - 1)S_m(n) \equiv mn\sum_{j=1}^{n-1}(aj)^{m-1}\left[\frac{aj}{n}\right] \pmod{n^2}.$$

Ultimately, from Theorem 2.3 we get the following Voronoï congruence:

Theorem 2.4. *Let $m \geq 2$ be even and $n \geq 1$. If $a \geq 1$ satisfies $(a,n) = 1$, then*

$$(a^m - 1)N_m \equiv mD_m\sum_{j=1}^{n-1}(aj)^{m-1}\left[\frac{aj}{n}\right] \pmod{n}.$$

The next one is known as the famous *von Staudt-Clausen theorem*.

Theorem 2.5. *Let p be a prime, m an even integer ≥ 2 and $\mathbb{Z}_p$ the ring of p-adic integers. If $p-1 \nmid m$, then $B_m \in \mathbb{Z}_p$. If $p-1 \mid m$, then $pB_m \in \mathbb{Z}_p$, precisely,*

$$pB_m \equiv p - 1 \pmod{p}. \tag{i}$$

More generally, if p is an odd prime and $m = k\varphi(p^s)$ $(k,s \geq 1)$, then

$$pB_m \equiv p - 1 \pmod{p^s}. \tag{ii}$$

Above congruence (i) describes an explicit shape of the denominator of B_m for an even integer $m \geq 2$. To be exact, B_m is expressed in the form

$$B_m = \omega(m) - \sum_{p-1|m}\frac{1}{p},$$

where $\omega(m)$ is an integer uniquely determined depending on m and the sum runs over all the primes p such that $p-1 \mid m$. On the one hand, congruence (ii) asserts that if $m = k\varphi(p^s)$ $(k,s \geq 1)$ for an odd prime p, then the above $\omega(m)$ satisfies

$$\omega(m) \equiv 1 + \sum_{\substack{q-1|m \\ q\neq p}}\frac{1}{q} \pmod{p^{s-1}}$$

with the sum taken over all the primes q such that $q-1 \mid m$ and $q \neq p$.

The congruences mentioned below are widely called *Kummer's congruences* for Bernoulli numbers. However, if we comply Slavutskii's request written in [15], it should be called *von Staudt-Kummer's congruences*, because von Staudt was the first contributor who discovered and investigated in details before Kummer.

Theorem 2.6. *Let p be an odd prime, m an even integer ≥ 2 and s an integer with $1 \leq s \leq m-1$. If $\beta_i(a) = (a^i - 1)\beta_i$ $(i \geq 1)$ for a positive integer a with $p \nmid a$, then*

$$\beta^m(a)\left(\beta^{p-1}(a)-1\right)^s \equiv 0 \pmod{p^s}. \tag{i}$$

In particular, if $p-1 \nmid m$, then

$$\beta^m\left(\beta^{p-1}-1\right)^s \equiv 0 \pmod{p^s}. \tag{ii}$$

The symbolic notation used in above congruences should be understood that we expand in full the left-hand side of (i) (resp. (ii)) using the binomial theorem and $\beta^i(a)$ (resp. β^i) is to be replaced by $\beta_i(a)$ (resp. β_i) for all $i = m + c(p-1)$, $c = 0, 1, ..., s$. That is, above (i) is exactly the same as the congruence

$$\sum_{c=0}^{s}(-1)^c\binom{s}{c}\beta_{m+c(p-1)}(a) \equiv 0 \pmod{p^s},$$

and also (ii) is the congruence exchanged here formally $\beta_{m+c(p-1)}(a)$ for $\beta_{m+c(p-1)}$.

Note that congruence (ii) is nothing but a special case of (i). In fact, taking a primitive root γ of p and choosing an integer $a \geq 1$ such that $a \equiv \gamma^{p^{s-1}} \pmod{p^s}$, we have $a^{p-1} \equiv \gamma^{\varphi(p^s)} \equiv 1 \pmod{p^s}$ by Euler's theorem. Since $p \nmid a$ and $p-1 \nmid m$, we also have $a^m \equiv a^{m+c(p-1)} \pmod{p^s}$ for each c and $a^m \not\equiv 1 \pmod{p}$. So, dividing (i) by $a^m - 1$, we can immediately deduce (ii).

Here, we would like to comment that a similar type congruence to above (ii) without any restriction on m has been obtained by von Staudt. For its explicit formula, see Slavutskii's article ((4) in [15]). Further, it should be noted that a sequence $\beta_i(a)$ $(i \geq 1)$ defined above is well-known to be the sequence of moments of a p-adic measure on the ring $\mathbb{Z}_p$.

The following theorem discovered by E. Lehmer [13] in 1939 was very important for the irregularity testing of primes for many years.

Theorem 2.7. *Let p be an odd prime and m be an even integer ≥ 2. Also put $Q_2(m) = 2^m - 1, Q_3(m) = \frac{1}{2}(3^m - 1), Q_4(m) = \frac{1}{2}(2^m - 1)(2^{m-1} - 1)$ and $Q_6(m) = \frac{1}{2}(6^{m-1} + 3^{m-1} + 2^{m-1} - 1)$. If $p-1 \nmid m-2$, then*

$$Q_k(m)\beta_m \equiv \sum_{0<i<p/k}(p-ik)^{m-1} \pmod{p^2},\ k = 2, 3, 4, 6,$$

provided that $p \geq 7$ for $k = 6$.

Applying the above congruence for $k = 2$, Lehmer showed that if $p-1 \nmid m-2$, then

$$2^{m-1}p\beta_m \equiv \frac{1}{m}\sum_{0<i<p/2}(p-2i)^m \pmod{p^3}.$$

We note that very simple and elegant p-adic proofs of above Lehmer's congruences were given by Johnson [11].

As mentioned in the Introduction, Jensen [10] investigated the distribution of irregular primes and proved in 1915 the following remarkable theorem.

Theorem 2.8. *There are infinitely many irregular primes p such that* $p \equiv 3 \pmod 4$.

A simple proof of the weaker theorem "*there are infinitely many irregular primes*" was given by Carlitz [6].

Recently, using multisectioning and convolution methods, Buhler *et al.* [5] determined all the irregular primes less than 12×10^6 and their irregular indices $i(p) = \#\{m \mid B_{2m} \equiv 0 \pmod p, 1 \le m \le (p-3)/2\}$.

3. Voronoï type congruences

In this section, we will first introduce some generalized Voronoï type congruences. As one of applications of these, we extend the von Staudt-Clausen congruences to more general situation. In addition, we study Giuga's conjecture by means of Bernoulli numbers.

For a positive integer n and an even integer $m \ge 2$, we define

$$\begin{aligned}\delta =&\delta(m,n) = \prod_{p|n} p^{u_p} \ \left(\text{where } u_p = \mathrm{ord}_p(m)\right),\\ \nu =&\nu(m,n) = \prod_{p|n} p^{\nu_p} \ \left(\text{where } \nu_p = \mathrm{ord}_p(D_m)\right).\end{aligned}$$

Particularly, if $n = 1$, then we put $\delta = \nu = 1$ by convention. Further, letting

$$\varepsilon_m(n) = \begin{cases} 1 & \text{if } n = 1,\\ \prod_{p|n}(1 - p^{m-1}) & \text{otherwise,}\end{cases}$$

we define, for an integer $a > 0$,

$$\begin{aligned} H_m(n) =&\varepsilon_m(n)\beta_m,\\ K_m(n;a) =&(a^m - 1)H_m(n) = \varepsilon_m(n)\beta_m(a),\\ H'_m(n) =&mH_m(n) = \varepsilon_m(n)B_m,\\ K'_m(n;a) =&(a^m - 1)H'_m(n) = \varepsilon_m(n)(a^m - 1)B_m.\end{aligned}$$

To deduce various important congruences for composite moduli, we introduce generalized Voronoï type congruences as follows:

Theorem 3.1. *Let $m \geq 2$ be even and $n \geq 1$. Also, let w and w' be arbitrary positive multiples of $n\delta\nu$ and $n\nu$, respectively. For a positive integer a with $(a,w) = (a,w') = 1$, we have*

$$K_m(n;a) \equiv \sum_{\substack{j=1\\(j,n)=1}}^{w-1} (aj)^{m-1} \left[\frac{aj}{w}\right] \pmod{n}, \tag{i}$$

$$K'_m(n;a) \equiv m \sum_{\substack{j=1\\(j,n)=1}}^{w'-1} (aj)^{m-1} \left[\frac{aj}{w'}\right] \pmod{n}. \tag{ii}$$

Proof. Since the proofs of (i) and (ii) are almost the same, we shall give below only the proof of (i). First, consider the Voronoï congruence in Theorem 2.4 replaced n by w:

$$(a^m - 1)N_m \equiv mD_m \sum_{j=1}^{w-1} (aj)^{m-1} \left[\frac{aj}{w}\right] \pmod{w}.$$

Since $(mD_m/\delta\nu, n) = 1$ and $w/\delta\nu \equiv 0 \pmod{n}$, dividing this by mD_m we get

$$(a^m - 1)\beta_m \equiv \sum_{j=1}^{w-1} (aj)^{m-1} \left[\frac{aj}{w}\right] \pmod{n}. \tag{3.1}$$

Here the sum on the right-hand side can be expressed as

$$\begin{aligned}\sum_{j=1}^{w-1} (aj)^{m-1} \left[\frac{aj}{w}\right] &= \sum_{\substack{j=1\\(j,n)=1}}^{w-1} (aj)^{m-1} \left[\frac{aj}{w}\right] + \sum_{\substack{j=1\\(j,n)\neq 1}}^{w-1} (aj)^{m-1} \left[\frac{aj}{w}\right] \\ &= \sum_{\substack{j=1\\(j,n)=1}}^{w-1} (aj)^{m-1} \left[\frac{aj}{w}\right] - \sum_{\substack{d|n\\d>1}} \mu(d)d^{m-1} \left(\sum_{j=1}^{w/d-1} (aj)^{m-1} \left[\frac{aj}{w/d}\right] \right),\end{aligned} \tag{3.2}$$

where μ is the Möbius function. Now consider congruence (3.1) replaced w by w/d, and multiply it by $\mu(d)d^{m-1}$. Then we have

$$\mu(d)d^{m-1}\beta_m(a) \equiv \mu(d)d^{m-1} \sum_{j=1}^{w/d-1} (aj)^{m-1} \left[\frac{aj}{w/d}\right] \pmod{n}.$$

Noting that $\varepsilon_m(n) = \sum_{d|n} \mu(d)d^{m-1}$ (where $\mu(1) = 1$), from (3.1) and (3.2)

$$K_m(n;a) = \left(1 + \sum_{\substack{d|n\\d>1}} \mu(d)d^{m-1}\right)\beta_m(a) \equiv \sum_{\substack{j=1\\(j,n)=1}}^{w-1} (aj)^{m-1} \left[\frac{aj}{w}\right] \pmod{n},$$

which is exactly congruence (i), as desired.

Theorem 3.2. *Let $m \geq 2$ be even and $n \geq 1$. Then*

$$nH'_m(n) \equiv \sum_{\substack{j=1 \\ (j,n)=1}}^{n-1} j^m \pmod{n}.$$

Proof. Using the similar method to that stated in the proof of Theorem 3.1, we express $S_m(n)$ as

$$S_m(n) = \sum_{\substack{j=1 \\ (j,n)=1}}^{n-1} j^m + \sum_{\substack{j=1 \\ (j,n)\neq 1}}^{n-1} j^m = \sum_{\substack{j=1 \\ (j,n)=1}}^{n-1} j^m - \sum_{\substack{d|n \\ d>1}} \mu(d)d^m \left(\sum_{j=1}^{n/d-1} j^m \right).$$

By Theorem 2.5 we see $\mathrm{ord}_p(D_m) \in \{0, 1\}$ for all prime divisors p of n, hence from Theorem 2.2 $S_m(n) \equiv nB_m \pmod{n}$ and $S_m(n/d) \equiv (n/d)B_m \pmod{n/d}$ for any positive divisor d of n. Multiplying the latter one by $\mu(d)d^m$, we have $\mu(d)d^m S_m(n/d) \equiv \mu(d)d^{m-1}nB_m \pmod{n}$. Substituting these congruences for every d into the above, it follows that

$$nH'_m(n) = \left(1 + \sum_{\substack{d|n \\ d>1}} \mu(d)d^{m-1} \right) nB_m \equiv \sum_{\substack{j=1 \\ (j,n)=1}}^{n-1} j^m \pmod{n},$$

which is precisely the congruence indicated.

With above notations, one can state

Corollary 3.3. *If $\varphi(n) \mid m$, then*

$$nH'_m(n) \equiv \varphi(n) \pmod{n}.$$

Proof. If $(j, n) = 1$ and $\varphi(n) \mid m$, then $j^m \equiv 1 \pmod{n}$. So the result follows immediately from Theorem 3.2.

Note that congruence (i) in Theorem 2.5 is given as a special case of Corollary 3.3 for the case $n = p$.

Let $\mathbb{Z}_n = \cap_{p|n}\mathbb{Z}_p$ $(n \geq 2)$ be the ring of rational numbers which are n-integral. Suppose that $m \geq 2$ is even and $\varphi(n) \mid m$. Writing as $B_m = \omega(m) + x_m + y_m$, where $\omega(m)$ is the integer mentioned in Section 2, $x_m \in \mathbb{Z}_n$ and $y_m \notin \mathbb{Z}_n$, we obviously see $y_m = -\sum_{p|n} 1/p$. On the one hand, the right-hand side of the congruence in Theorem 3.2 is unchanged modulo n even if we replace m by $l \geq 2$ satisfying $m \equiv l \pmod{\varphi(n)}$. Therefore, if $m \equiv l \pmod{\varphi(n)}$ for $n \geq 3$, then we have

$$nH'_m(n) \equiv nH'_l(n) \pmod{n}.$$

However, since $B_m \in \mathbb{Z}_n$ if and only if $B_l \in \mathbb{Z}_n$, this congruence is interesting only in the case $B_m \notin \mathbb{Z}_n$.

As recurrence relations for $H'_m(n)$, we can give the following

Theorem 3.4. *Let $m \geq 1, n \geq 2$ and $a \geq 1$ be integers with $(a,n) = 1$. Then*

$$\big(H'(n)+n\big)^{m+1} - H^{'m+1}(n) = (m+1) \sum_{\substack{j=1 \\ (j,n)=1}}^{n-1} j^m, \tag{i}$$

$$\begin{aligned}&(a^m-1)\Big\{\big(H'(n)+n\big)^{m+1} - H^{'m+1}(n)\Big\} \\ &=(m+1)\sum_{i=1}^{m}(-1)^{i+1}\binom{m}{i}n^i \sum_{\substack{j=1 \\ (j,n)=1}}^{n-1} (aj)^{m-i}\left[\frac{aj}{n}\right]^i .\end{aligned} \tag{ii}$$

We do not give the proof of this theorem, because both congruences (i) and (ii) are nothing but special cases of known formulas for generalized Bernoulli numbers (see Theorems 1 and 3 in Agoh [1]). In addition, we note that Theorem 3.2 can be also derived from above (i).

Now, we would like to introduce an interesting problem related to a characterization of primes, which is deeply related to the von Staudt-Clausen congruence. Put

$$G = \{n \geq 2 \mid S_{n-1}(n) \equiv n-1 \ (\mathrm{mod}\ n)\}.$$

By Fermat's little theorem, it is clear that the set G contains any primes. In 1950, Giuga [8] conjectured that G is precisely the same as the set of all the primes. By elementary observation, we see that the following statements are all equivalent (for details, see Agoh [2], Borwein *et al.* [4] and Kellner [12]):

(a) $n \in G$,

(b) $p^2(p-1) \mid n-p$ for any prime divisor p of n,

(c) $nB_{n-1} \equiv n-1 \ (\mathrm{mod}\ n)$.

Therefore, we can restate Giuga's conjecture as follows:

Conjecture 3.5. *Let $n \geq 2$. Then $nB_{n-1} \equiv n-1 \ (\mathrm{mod}\ n)$ if and only if n is a prime.*

A composite n is called a *Carmichael number* if $a^{n-1} \equiv 1 \ (\mathrm{mod}\ n)$ for every positive integer a with $(a,n) = 1$. Such the smallest number is $561 = 3 \cdot 11 \cdot 17$. It is easily shown that n is a Carmichael number if and only if $n = p_1 p_2 \cdots p_g$ (the product of some distinct odd primes) and $p(p-1) \mid n-p$ for each prime divisor p of n. Further, this number may be characterized by $nB_{n-1} \equiv -n\sum_{p|n} 1/p \ (\mathrm{mod}\ n)$. In their outstanding paper [3], Alford, Granville and Pomerance proved that there exist infinitely many Carmichael numbers. We can show that if there is a composite number $n \in G$, then n is the Carmichael number and the number of its prime divisors must be greater than the smallest prime divisor of n.

Also we can say that if $n \in G$ is composite, then (cf. Agoh [2])

$$\begin{cases} pB_{n-p} \equiv p-1 \ (\mathrm{mod}\ p^3), \\ pB_{(n/p)-1} \equiv p-1 \ (\mathrm{mod}\ p^2), \\ pB_{((n/p)-1)/p} \equiv p-1 \ (\mathrm{mod}\ p) \end{cases}$$

for all prime divisors p of n.

It is unknown whether there is a composite number n belonging to G. Recently, it was shown in Borwein *et al.* [4] that any counter example has at least 12055 digits. For more extensive computations, see Fee and Plouffe [7]. If it is possible to appreciate the justification of the above conjecture, then an interesting characterization of primes can be given by means of the Bernoulli number.

4. Generalized von Staudt-Kummer congruences

In this section, we will generalize von Staudt-Kummer congruences stated in Theorem 2.6.

In what follows, we assume that n, s, m_r, a_r, b_r $(r = 1, 2, ..., k)$ are positive integers with $n \geq 3$ and $(a_r, n) = 1$.

Theorem 4.1. *For each $r = 1, 2, ..., k+1$, we assume that m_r is even and $\lambda_r \in \mathbb{Z}_n$ satisfies $\sum_{i=1}^{k+1} \lambda_i \equiv 0 (\text{mod } n)$. Then we have*

$$\prod_{r=1}^{k} K^{m_r}(n; a_r) \left(\sum_{r=1}^{k} \lambda_r K^{b_r \varphi(n)}(n; a_r) + \lambda_{k+1} \right)^s \equiv 0 \ (\text{mod } n^s). \tag{i}$$

In particular, if $n = p^\alpha$ ($\alpha \geq 1, p$ an odd prime) and $p - 1 \nmid m_r$, $r = 1, 2, ..., k$, then

$$\prod_{r=1}^{k} H_r^{m_r}(n) \left(\sum_{r=1}^{k} \lambda_r H_r^{b_r \varphi(n)}(n) + \lambda_{k+1} \right)^s \equiv 0 \ (\text{mod } n^s). \tag{ii}$$

The symbolic expression used in the above statement means that we expand the left-hand side of (i) (resp. (ii)) in full by making use of the multinomial theorem regarding the K's (resp. H's) as ordinary real numbers, and afterwards, $K^l(n; a_r)$ (resp. $H_r^l(n)$) is to be replaced by $K_l(n; a_r)$ (resp. $H_l(n)$) for each r.

Proof. Since $n \geq 3$, we know that all of $m_r + cb_r\varphi(n)$ for $r = 1, 2, ..., k$ and $c = 0, 1, ..., s$ are even. Also, it follows that $p - 1 \mid m_r$ if and only if $p - 1 \mid m_r + cb_r\varphi(n)$ for each prime divisor p of n, hence $\text{ord}_p(D_{m_r}) = \text{ord}_p(D_{m_r + cb_r\varphi(n)})$. We now put

$$\xi = n^s \prod_{p \mid n} p^{f_p + g_p},$$

where

$$f_p = \max_{\substack{1 \leq r \leq k \\ 0 \leq c \leq s}} \left\{ \text{ord}_p(m_r + cb_r\varphi(n)) \right\} \quad \text{and} \quad g_p = \max_{1 \leq r \leq k} \left\{ \text{ord}_p(D_{m_r}) \right\}.$$

Noticing that m and n can be chosen independently, we may consider congruence (i) in Theorem 3.1 which is replaced a, m, n and w by $a_r, m_r + cb_r\varphi(n), n^s$ and ξ, respectively:

$$K_{m_r + cb_r\varphi(n)}(n; a_r) \equiv \sum_{\substack{j_r = 1 \\ (j_r, n) = 1}}^{\xi - 1} (a_r j_r)^{m_r + cb_r\varphi(n) - 1} \left[\frac{a_r j_r}{\xi} \right] \ (\text{mod } n^s),$$

which is valid for all $r = 1,2,\dots,k$ and $c = 0,1,\dots,s$. Making use of this congruence, we can deduce the following

$$\begin{aligned}
&\prod_{r=1}^{k} K^{m_r}(n;a_r)\left(\sum_{r=1}^{k}\lambda_r K^{b_r\varphi(n)}(n;a_r)+\lambda_{k+1}\right)^{s}\\
&=\sum_{\substack{0\le c_1,\dots,c_{k+1}\le s\\ c_1+\cdots+c_{k+1}=s}}\binom{s}{c_1,\dots,c_{k+1}}\left(\prod_{r=1}^{k}\lambda_r^{c_r}K_{m_r+c_rb_r\varphi(n)}(n;a_r)\right)\lambda_{k+1}^{c_{k+1}}\\
&\equiv\sum_{\substack{0\le c_1,\dots,c_{k+1}\le s\\ c_1+\cdots+c_{k+1}=s}}\binom{s}{c_1,\dots,c_{k+1}}\left(\prod_{r=1}^{k}\left(\lambda_r^{c_r}\sum_{\substack{j_r=1\\(j_r,n)=1}}^{\xi-1}(a_rj_r)^{m_r+c_rb_r\varphi(n)-1}\left[\frac{a_rj_r}{\xi}\right]\right)\right)\lambda_{k+1}^{c_{k+1}}\\
&\equiv\sum_{\substack{j_1=1\\(j_1,n)=1}}^{\xi-1}\cdots\sum_{\substack{j_k=1\\(j_k,n)=1}}^{\xi-1}\left\{\sum_{\substack{0\le c_1,\dots,c_{k+1}\le s\\ c_1+\cdots+c_{k+1}=s}}\binom{s}{c_1,\dots,c_{k+1}}\right.\\
&\qquad\qquad\qquad\left.\times\left(\prod_{r=1}^{k}\lambda_r^{c_r}(a_rj_r)^{m_r+c_rb_r\varphi(n)-1}\left[\frac{a_rj_r}{\xi}\right]\right)\lambda_{k+1}^{c_{k+1}}\right\}\\
&\equiv\sum_{\substack{j_1=1\\(j_1,n)=1}}^{\xi-1}\cdots\sum_{\substack{j_k=1\\(j_k,n)=1}}^{\xi-1}\left\{\left(\sum_{r=1}^{k}\lambda_r(a_rj_r)^{b_r\varphi(n)}+\lambda_{k+1}\right)^{s}\prod_{r=1}^{k}(a_rj_r)^{m_r-1}\left[\frac{a_rj_r}{\xi}\right]\right\}\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\pmod{n^s}.
\end{aligned}$$

Since $(a_rj_r,n)=1$ for each r, under the assumption for the λ's we have

$$\sum_{r=1}^{k}\lambda_r(a_rj_r)^{b_r\varphi(n)}+\lambda_{k+1}\equiv\sum_{i=1}^{k+1}\lambda_i\equiv 0 \pmod{n},$$

which offers congruence (i) as desired.

Next, assume that $n=p^{\alpha}$ ($\alpha\ge 1, p$ an odd prime) and $p-1\nmid m_r$ ($r=1,2,\dots,k$). In this case, n has a primitive root γ, so take a positive integer a with $a\equiv\gamma^{n^{s-1}} \pmod{n^s}$. Then, by Euler's theorem we see $a^{\varphi(n)}\equiv\gamma^{n^{s-1}\varphi(n)}\equiv\gamma^{\varphi(n^s)}\equiv 1 \pmod{n^s}$. Now choose especially $a_1=a_2=\cdots=a_k=a$ in (i). Then $a^{c\varphi(n)}\equiv 1 \pmod{n^s}$ for any $c\ge 0$ and $(a^{m_r}-1,n)=1$ for each r. Dividing (i) by $\prod_{r=1}^{k}(a^{m_r}-1)$, we can deduce (ii) immediately.

With above notations, we have

Corollary 4.2. *Let p be an odd prime, $m_r\ge s+1$ for $r=1,2,\dots,k$ and assume that $\lambda_i\in\mathbb{Z}_p$ ($i=1,2,\dots,k+1$) satisfy $\sum_{i=1}^{k+1}\lambda_i\equiv 0$(mod p). Then*

$$\prod_{r=1}^{k}\beta_r^{m_r}(a_r)\left(\sum_{r=1}^{k}\lambda_r\beta_r^{b_r(p-1)}(a_r)+\lambda_{k+1}\right)^{s}\equiv 0 \pmod{p^s}. \qquad \text{(i)}$$

In particular, if $p-1 \nmid m_r$ $(r=1,2,...,k)$*, then*

$$\prod_{r=1}^{k} \beta_r^{m_r} \left(\sum_{r=1}^{k} \lambda_r \beta_r^{b_r(p-1)} + \lambda_{k+1} \right)^s \equiv 0 \pmod{p^s}. \tag{ii}$$

It may be unnecessary to comment on the symbolic notation used in the above corollary, but we want to explain it once more to make doubly sure. Above congruence (i) means that we calculate the left-hand side of (i) in full regarding $\beta_r(a_r)$ $(r=1,2,...,k)$ as ordinary real numbers, and replace $\beta_r^{g(r)}(a_r)$ by $\beta_{g(r)}(a_r)$ for each r and various values of $g(r)$. Hence, (i) is precisely the same as

$$\sum_{\substack{0 \le c_1,...,c_k \le s \\ c_1+\cdots+c_{k+1}=s}} \binom{s}{c_1,...,c_{k+1}} \left(\prod_{r=1}^{k} \lambda_r^{c_r} \beta_{m_r+c_r b_r(p-1)}(a_r) \right) \lambda_{k+1}^{c_{k+1}} \equiv 0 \pmod{p^s}.$$

We do not say fully, but the symbolic notation used in (ii) should be also understood similarly to that used in (i).

Proof. Take $n=p$ in Theorem 4.1. Since $m_r - 1 \ge s$ for each r, we get $\varepsilon_{m_r}(p^s) = 1 - p^{m_r-1} \equiv 1 \pmod{p^s}$, so that $H_{m_r}(p^s)(a_r) \equiv \beta_{m_r}(a_r) \pmod{p^s}$. Additionally, if $p-1 \nmid m_r$ $(r=1,2,...,k)$, then we can choose a positive integer a with $(a^{m_r}-1,p)=1$ for each r. Therefore, using the same methods as in the proof of Theorem 4.1, we get the indicated congruences.

As a special case of Corollary 4.2, we may state the following

Corollary 4.3. *Let* p *be an odd prime,* $s,b \ge 1$*,* m *be an even integer* ≥ 2*,* $m \ge s+1$ *and assume that* $\lambda_1, \lambda_2 \in \mathbb{Z}_p$ *satisfy* $\lambda_1 + \lambda_2 \equiv 0 \pmod{p}$*. If* a *is a positive integer with* $(a,p)=1$*, then*

$$\beta^m(a) \left(\lambda_1 \beta^{b(p-1)}(a) + \lambda_2 \right)^s \equiv 0 \pmod{p^s}. \tag{i}$$

In particular, if $p-1 \nmid m$*, then*

$$\beta^m \left(\lambda_1 \beta^{b(p-1)} + \lambda_2 \right)^s \equiv 0 \pmod{p^s}. \tag{ii}$$

Proof. Take $k=1$ in Corollary 4.2.

Choosing especially $b=\lambda_1=1$ and $\lambda_2=-1$ in the above corollary, we can derive readily Theorem 2.6.

Corollary 4.4. *Let* m *be an even integer* ≥ 2*,* n,a *be positive integers with* $(a,n)=1$ *and* $n \ge 3$*. If* $m \equiv l \pmod{\varphi(n)}$ *for* $l \ge 2$*, then*

$$K_m(n;a) \equiv K_l(n;a) \pmod{n}. \tag{i}$$

In particular, if p *is an odd prime with* $p-1 \nmid m$ *and* $m \equiv l \pmod{\varphi(p^\alpha)}$ $(\alpha \ge 1)$ *for* $l \ge 2$*, then*

$$H_m(p) \equiv H_l(p) \pmod{p^\alpha}. \tag{ii}$$

Proof. Take $s = k = \lambda_1 = 1$ and $\lambda_2 = -1$ in Theorem 4.1 and note that $H_i(p^\alpha) = H_i(p)$ for any $i \geq 1$. Then, congruence (i) and (ii) are immediate.

Let n, a be positive integers with $n \geq 3$ and $(a, n) = 1$, and let s, b be positive integers. Then we obtain

Theorem 4.5. *Let $m \geq 2$ be an even integer and assume that $\lambda_1, \lambda_2 \in \mathbb{Z}_n$ satisfy $\lambda_1 + \lambda_2 \equiv 0 \pmod{n}$. Then*

$$K'^{m}(n;a)\left(\lambda_1 K'^{b\varphi(n)}(n;a) + \lambda_2\right)^s \equiv 0 \pmod{n^{s-1}}. \tag{i}$$

In particular, if $n = p^\alpha$ ($\alpha \geq 1$, p an odd prime), $p - 1 \nmid m$ and $\lambda_1, \lambda_2 \in \mathbb{Z}_p$ satisfy $\lambda_1 + \lambda_2 \equiv 0 \pmod{p}$, then

$$H'^{m}(n)\left(\lambda_1 H'^{b\varphi(n)}(n) + \lambda_2\right)^s \equiv 0 \pmod{n^{s-1}}. \tag{ii}$$

Proof. As defined in Section 3, let $\nu = \prod_{p|n} p^{\nu_p}$ (where $\nu_p = \mathrm{ord}_p(D_m)$) and put $\eta = n^s\nu$. Since $\mathrm{ord}_p(D_m) = \mathrm{ord}_p(D_{m+cb\varphi(n)})$ for each prime divisor p of n and $c = 0, 1, ..., s$, we may consider the Voronoï type congruence (ii) in Theorem 3.1 replaced m, n and w' by $m + cb\varphi(n), n^s$ and η, respectively. Noting that $\varepsilon_m(n^s) = \varepsilon_m(n)$ and hence $K'_m(n^s; a) = K'_m(n; a)$ for any m, we have

$$K'_{m+cb\varphi(n)}(n;a) \equiv (m + cb\varphi(n)) \sum_{\substack{j=1 \\ (j,n)=1}}^{\eta-1} (aj)^{m+cb\varphi(n)-1} \left[\frac{aj}{\eta}\right] \pmod{n^s}.$$

Using this congruence, it follows that

$$\begin{aligned}
K'^{m}(n;a)\left(\lambda_1 K'^{b\varphi(n)}(n;a) + \lambda_2\right)^s &= \sum_{c=0}^{s} \binom{s}{c} \lambda_1^c K'_{m+cb\varphi(n)}(n;a) \lambda_2^{s-c} \\
\equiv & \sum_{c=0}^{s} \binom{s}{c} \lambda_1^c \lambda_2^{s-c} \left((m + cb\varphi(n)) \sum_{\substack{j=1 \\ (j,n)=1}}^{\eta-1} (aj)^{m+cb\varphi(n)-1} \left[\frac{aj}{\eta}\right] \right) \\
\equiv & \sum_{c=0}^{s} \binom{s}{c} \lambda_1^c \lambda_2^{s-c} \left(m \sum_{\substack{j=1 \\ (j,n)=1}}^{\eta-1} (aj)^{m+cb\varphi(n)-1} \left[\frac{aj}{\eta}\right] \right) \\
& + \sum_{c=0}^{s} \binom{s}{c} \lambda_1^c \lambda_2^{s-c} \left(cb\varphi(n) \sum_{\substack{j=1 \\ (j,n)=1}}^{\eta-1} (aj)^{m+cb\varphi(n)-1} \left[\frac{aj}{\eta}\right] \right) \\
\equiv & m \sum_{\substack{j=1 \\ (j,n)=1}}^{\eta-1} (aj)^{m-1} \left(\sum_{c=0}^{s} \binom{s}{c} \lambda_1^c \lambda_2^{s-c} (aj)^{cb\varphi(n)} \right) \left[\frac{aj}{\eta}\right] \\
& + s\lambda_1 b\varphi(n) \sum_{\substack{j=1 \\ (j,n)=1}}^{\eta-1} (aj)^{m+b\varphi(n)-1} \left(\sum_{c'=0}^{s} \binom{s-1}{c'} \lambda_1^{c'} \lambda_2^{s-1-c'} (aj)^{c'b\varphi(n)} \right) \left[\frac{aj}{\eta}\right]
\end{aligned}$$

$$\equiv m \sum_{\substack{j=1\\(j,n)=1}}^{\eta-1} (aj)^{m-1} \left(\lambda_1 (aj)^{b\varphi(n)} + \lambda_2\right)^s \left[\frac{aj}{\eta}\right]$$

$$+ s\lambda_1 b\varphi(n) \sum_{\substack{j=1\\(j,n)=1}}^{\eta-1} (aj)^{m+b\varphi(n)-1} \left(\lambda_1 (aj)^{b\varphi(n)} + \lambda_2\right)^{s-1} \left[\frac{aj}{\eta}\right] \pmod{n^s}.$$

Since $(aj)^{b\varphi(n)} \equiv 1 \pmod{n}$ if $(aj,n) = 1$, we have, for $\kappa = s, s-1$,

$$\left(\lambda_1 (aj)^{b\varphi(n)} + \lambda_2\right)^\kappa \equiv (\lambda_1 + \lambda_2)^\kappa \equiv 0 \pmod{n^{s-1}}.$$

From this congruence we can readily derive (i). When $p-1 \nmid m$, (ii) can be easily given from (i) by the same arguments as done for the proof of (ii) in Theorem 4.1.

Using the same notations as in Theorem 4.5, we can state

Corollary 4.6. *Let p be an odd prime and assume that $\lambda_1, \lambda_2 \in \mathbb{Z}_p$ satisfy $\lambda_1 + \lambda_2 \equiv 0 \pmod{p}$. If $m \geq s$ and $\beta_i'(a) = i\beta_i(a) = (a^i - 1)B_i$ $(i \geq 1)$, then*

$$\beta'^m(a)\left(\lambda_1 \beta'^{b(p-1)}(a) + \lambda_2\right)^s \equiv 0 \pmod{p^{s-1}}. \tag{i}$$

In particular, if $p-1 \nmid m$, then

$$B^m\left(\lambda_1 B^{b(p-1)} + \lambda_2\right)^s \equiv 0 \pmod{p^{s-1}}. \tag{ii}$$

Proof. Since $m \geq s$, we see $\varepsilon_m(p) = 1 - p^{m-1} \equiv 1 \pmod{p^{s-1}}$, and so the corollary follows from Theorem 4.5.

To obtain some generalized von Staudt-Kummer congruences in this section, we made use of Voronoï type congruences stated in Section 3. However, besides our method, there are other sagacious ones to accomplish the purpose. Indeed, two sequences $H_m(n)$ and $K_m(n;a)$ ($m \geq 2$, even) defined in Section 3 are the moments of p-adic measures on the unit group $\mathbb{Z}_p^\times$ of $\mathbb{Z}_p$ and this realization brings us the congruences such as Theorem 4.1 (cf., e.g., Young [18, 19]). For the other method obtaining extended Voronoï and von Staudt-Kummer congruences, see Sun's interesting approach in [16].

5. Generalization of Lehmer's congruences

In this section, we will extend Lehmer's congruences in Theorem 2.7 to more general moduli.

Assume that $m \geq 2$ is even and $p-1 \nmid m-2$ for all prime divisors p of n. Then we have $m \neq 2$ (hence $m \geq 4$) and $B_{m-2} \in \mathbb{Z}_p$. Also it is clear that $2 \nmid n$ and $3 \nmid n$, hence $p \geq 5$. Recall the Euler-MacLaurin summation formula (Theorem 2.2) and observe each term on the right-hand side of this formula. For simplicity, we put

$$X_j = \frac{1}{j}\binom{m}{j-1} B_{m+1-j} n^j \quad \text{for} \quad j = 1, 2, \ldots, m+1.$$

If j is an even integer with $m-2 \geq j \geq 2$, then $X_j = 0$. So we observe here only the terms X_j with $j = 2i+1\,(i = 0, 1, ..., m/2)$ and $j = m$.

Let p be any prime divisor of n. If $m > 2i \geq 4$, then $\mathrm{ord}_p(D_{m-2i}) \in \{0, 1\}$ and $p^{2i-3} \geq 5^{2i-3} \geq 2i+1$, hence $\mathrm{ord}_p\left(X_{2i+1}\right) \geq -(2i-3) - 1 + (2i+1) = 3$. This gives $X_{2i+1} \equiv 0 \pmod{n^3}$ for all $i \geq 2$. Also, since $\mathrm{ord}_p(D_{m-2}) = 0$ by the assumption, $m \geq 4$ and $(n, 6) = 1$, it follows that $X_3 = \frac{1}{3}\binom{m}{2}B_{m-2}n^3 \equiv 0 \pmod{n^3}$ and $X_m = \frac{1}{m}\binom{m}{m-1}B_1 n^m = -\frac{1}{2}n^m \equiv 0 \pmod{n^3}$. Consequently, we get from Theorem 2.2

$$S_m(n) \equiv B_m n \pmod{n^3}.$$

On the other hand, we obtain from (2.1) that if $(a, n) = 1$, $a \geq 1$, then

$$(a^m - 1)S_m(n) \equiv mn\sum_{j=1}^{n-1}(aj)^{m-1}\left[\frac{aj}{n}\right] - \frac{m(m-1)}{2}n^2\sum_{j=1}^{n-1}(aj)^{m-2}\left[\frac{aj}{n}\right]^2 \pmod{n^3}.$$

Consequently, we have

$$(a^m - 1)B_m \equiv m\sum_{j=1}^{n-1}(aj)^{m-1}\left[\frac{aj}{n}\right] - \frac{m(m-1)}{2}n\sum_{j=1}^{n-1}(aj)^{m-2}\left[\frac{aj}{n}\right]^2 \pmod{n^2}.$$

Let δ be as in Section 2 and set $\eta' = n\delta$. Since $(a, \eta') = 1$, we may consider the above congruence replaced n by η'. That is,

$$(a^m - 1)B_m \equiv m\sum_{j=1}^{\eta'-1}(aj)^{m-1}\left[\frac{aj}{\eta'}\right] - \frac{m(m-1)}{2}\eta'\sum_{j=1}^{\eta'-1}(aj)^{m-2}\left[\frac{aj}{\eta'}\right]^2 \pmod{\eta'^2},$$

which implies

$$(a^m - 1)\beta_m \equiv \sum_{j=1}^{\eta'-1}(aj)^{m-1}\left[\frac{aj}{\eta'}\right] - \frac{m-1}{2}\eta'\sum_{j=1}^{\eta'-1}(aj)^{m-2}\left[\frac{aj}{\eta'}\right]^2 \pmod{n^2}. \tag{5.1}$$

Putting, for $i = 0, 1, ..., a-1$,

$$G_i^{(a)} = \left\{ j \in \mathbb{Z} \mid \frac{i\eta'}{a} < j < \frac{(i+1)\eta'}{a} \right\},$$

and

$$U_i^{(a)} = \sum_{j \in G_i^{(a)}} j^{m-1}, \quad V_i^{(a)} = \sum_{j \in G_i^{(a)}} j^{m-2},$$

above (5.1) can be expressed as

$$(a^m - 1)\,\beta_m \equiv a^{m-1}\sum_{i=1}^{a-1} iU_i^{(a)} - \frac{m-1}{2}a^{m-2}\eta'\sum_{i=1}^{a-1} i^2 V_i^{(a)} \pmod{n^2}. \tag{5.2}$$

On the other hand, since m is even, it follows that

$$\begin{aligned} U_i^{(a)} = \sum_{j\in G_{a-1-i}^{(a)}} (\eta'-j)^{m-1} &\equiv - \sum_{j\in G_{a-1-i}^{(a)}} j^{m-1} + (m-1)\eta' \sum_{j\in G_{a-1-i}^{(a)}} j^{m-2} \\ &\equiv - U_{a-1-i}^{(a)} + (m-1)\eta' V_{a-1-i}^{(a)} \pmod{n^2}. \end{aligned}$$

We also have

$$V_i^{(a)} = \sum_{j\in G_{a-1-i}^{(a)}} (\eta'-j)^{m-2} \equiv \sum_{j\in G_{a-1-i}^{(a)}} j^{m-2} \equiv V_{a-1-i}^{(a)} \pmod{n}.$$

By Theorem 2.2 we see, since $B_{m-2} \in \mathbb{Z}_p$ for any prime divisor p of n such that $p-1 \nmid m-2$,

$$S_{m-2}(\eta') = \sum_{i=0}^{a-1} V_i^{(a)} \equiv 0 \pmod{n}.$$

We are now able to prove the following generalizations of Lehmer's congruences stated in Theorem 2.7.

Theorem 5.1. *Let n be an odd integer, m an even integer ≥ 2, $\eta' = n\delta$, and let $Q_k(m)$ $(k = 2,3,4,6)$ be as mentioned in Theorem 2.7. If $p-1 \nmid m-2$ for every prime divisor p of n, then*

$$Q_k(m)\beta_m \equiv \sum_{0<j<\eta'/k} (\eta' - kj)^{m-1} \pmod{n^2},\ k = 2,3,4,6, \tag{5.3}$$

provided that every prime divisor p of n is ≥ 7 when $k = 6$.

Proof. Since each proof of (5.3) for $k = 2,3,4,6$ is similar, we give only the proof for $k = 6$, under the assumption that (5.3) holds for $k = 2,3$. In here and what follows, we write $U_i = U_i^{(6)}$ and $V_i = V_i^{(6)}$ $(i = 0,1,...,5)$ for simplification.

From the congruences mentioned above we get $U_i \equiv -U_{5-i} + (m-1)\eta' V_{5-i} \pmod{n^2}$ and $V_i \equiv V_{5-i} \pmod{n}$ for $i = 3,4,5$. Since $(n,6) = 1$, by taking $a = 6$ in (5.2), we obtain

$$\begin{aligned} (6^m - 1)\beta_m \equiv & 6^{m-1}\sum_{i=1}^{5} iU_i - \frac{m-1}{2} 6^{m-2}\eta' \sum_{i=1}^{5} i^2 V_i \\ \equiv & -6^{m-1}(5U_0 + 3U_1 + U_2) + \frac{m-1}{2} 6^{m-2}\eta'(35V_0 + 31V_1 + 23V_2) \\ & \pmod{n^2}. \end{aligned}$$

Under the given condition, $B_{m-2} \in \mathbb{Z}_p$ for every prime divisor p of n, so we get $\sum_{i=0}^{5} V_i \equiv 2\left(V_0 + V_1 + V_2\right) \equiv 0 \pmod{n}$, which implies $V_2 \equiv -V_0 - V_1 \pmod{n}$ since n is odd. Consequently, dividing the above congruence by 6^{m-1} we have

$$(6 - 6^{1-m})\beta_m \equiv -(5U_0 + 3U_1 + U_2) + \frac{m-1}{3}\eta'(3V_0 + 2V_1) \pmod{n^2}.$$

Assume that (5.3) holds for $k = 2$ and 3, i.e., in equivalent forms

$$\begin{aligned}(2-2^{1-m})\beta_m \equiv& -(U_0+U_1+U_2)+\frac{m-1}{2}\eta'(V_0+V_1+V_2)\\ \equiv& -(U_0+U_1+U_2) \pmod{n^2},\\ (3-3^{1-m})\beta_m \equiv& -2(U_0+U_1)+\frac{2(m-1)}{3}\eta'(V_0+V_1) \pmod{n^2}.\end{aligned}$$

Combining these congruences, we deduce

$$\begin{aligned}(1+2^{1-m}+3^{1-m}-6^{1-m})\beta_m =& \left\{-(2-2^{1-m})-(3-3^{1-m})+(6-6^{1-m})\right\}\beta_m\\ \equiv& -2U_0+\frac{m-1}{3}\eta' V_0 \pmod{n^2},\end{aligned}$$

that is,

$$\begin{aligned}(6^{m-1}+3^{m-1}+2^{m-1}-1)\beta_m \equiv& 2\left(-6^{m-1}U_0+(m-1)6^{m-2}\eta' V_0\right)\\ \equiv& 2\sum_{j\in G_0^{(6)}}(\eta'-6j)^{m-1} \pmod{n^2},\end{aligned}$$

which completes the proof of (5.3) for $k = 6$.

6. Properties of the numerator of β_m

In this final section, we would like to discuss some basic properties of the numerator of β_m for an even integer $m \geq 2$.

As defined in Section 2, let N'_m be the numerator of β_m.

Theorem 6.1. *Let $n = p_1p_2\cdots p_s$ be the product of some distinct irregular primes such that $(\frac{1}{2}(p_i-1), \frac{1}{2}(p_j-1)) = 1$ for every $i, j = 1, 2, \ldots, s$ with $i \neq j$. Then there exists an even integer $m \geq 2$ such that $N'_m \equiv 0 \pmod{n}$.*

Proof. Since all the primes p_i, $i = 1, 2, \ldots, s$, are irregular, there exist even integers $2m_i$, $1 \leq m_i \leq \frac{1}{2}(p_i-3)$, such that $B_{2m_i} \equiv 0 \pmod{p_i}$. Since $(\frac{1}{2}(p_i-1), \frac{1}{2}(p_j-1)) = 1$ if $i \neq j$, by the Chinese remainder theorem the system of congruences

$$X \equiv m_i \pmod{\tfrac{1}{2}(p_i-1)}, \quad i = 1, 2, \ldots, s,$$

has uniquely the solution $X = \alpha > 0$ modulo $\frac{1}{2^s}\prod_{i=1}^{s}(p_i-1)$ in common. If we choose $m = 2\alpha$, then $p_i - 1 \nmid m$ and $\beta_m \equiv \beta_{2m_i} \equiv 0 \pmod{p_i}$ by Theorem 2.6, which are valid for all $i = 1, 2, \ldots, s$. This completes the proof.

It is evident that if n is divisible by at least two distinct irregular primes p and q with $(\frac{1}{2}(p-1), \frac{1}{2}(q-1)) \neq 1$, then there does not exist an even integer $m \geq 2$ such that $N'_m \equiv 0 \pmod{n}$.

We shall give here an example of Theorem 6.1 for $n = 37 \cdot 59 \cdot 131$, the product of three irregular primes satisfying the indicated condition. All the irregularity indices of 37, 59 and

131 are equal to 1 and the corresponding irregular pairs $(p, 2m)$ satisfying $B_{2m} \equiv 0 \pmod{p}$ $(1 \le m \le (p-3)/2)$ are $(37,32), (59,44)$ and $(131,22)$, respectively. So consider the system of congruences

$$X \equiv 16 \pmod{18},\ X \equiv 22 \pmod{29},\ X \equiv 11 \pmod{65}.$$

Then we find the common solution $X \equiv 2806 \pmod{18 \cdot 29 \cdot 65}$ and therefore, letting $m = 2 \cdot 2806 = 5612$, we have $N'_m \equiv 0 \pmod{37 \cdot 59 \cdot 131}$.

Let $n \ge 3$ and $\varepsilon_m(n)$ (m an even integer ≥ 2) be as in Section 3. If $m \equiv l \pmod{\varphi(n)}$ for $m, l \ge 2$, then we know that $(\varepsilon_m(n), n) = d$ if and only if $(\varepsilon_l(n), n) = d$. If $p - 1 \nmid m$ for all prime divisors p of n, then $H_m(n) \equiv H_l(n) \pmod{n}$ by Corollary 4.3, hence putting $n_0 = n/d$, we have

$$\frac{\varepsilon_m(n)}{d}\beta_m \equiv \frac{\varepsilon_l(n)}{d}\beta_l \pmod{n_0},$$

where $(\varepsilon_m(n)/d, n_0) = (\varepsilon_l(n)/d, n_0) = 1$. Consequently, if $m \equiv l \pmod{\varphi(n)}$, then $(N'_m, n_0) = (N'_l, n_0)$. Here we see $p-1 \nmid m$ for any prime divisor p of N'_m. Indeed, if $p-1 \mid m$, then $B_m \notin \mathbb{Z}_p$ by Theorem 2.5, which is contrary to $(N'_m, D'_m) = 1$. In particular, taking $n = |N'_m| > 3$ and $d = (\varepsilon_m(n), N'_m)$, it is easily seen that if $m \equiv l \pmod{\varphi(N'_m)}$, then $|N'_m/d| = (N'_l, N'_m/d)$.

The next theorem can be deduced immediately from Theorem 2.8, however we would like to give the proof from a different viewpoint without of use primes.

Theorem 6.2. *The set* $\mathscr{S} = \{|N'_{2m}| \mid m = 1,2,3,...\}$ *contains infinitely many elements that are relatively prime in pairs.*

Proof. Assume that $|N'_{2m_1}|, |N'_{2m_2}|, ..., |N'_{2m_k}|$ are all the elements in $\mathscr{S}$ which are relatively prime in pairs. Since $|\beta_{2m}| \to \infty$ as $m \to \infty$, we can choose $x \ge 1$ such that $\varphi(M_1) \ge 6$ and $|\beta_{\varphi(M_1)}| > 1$ for $M_1 = x\prod_{i=1}^{k}|N'_{2m_i}|$. Then we see from Theorem 2.5 that $\prod_{p|M_1} p$ divides $D'_{\varphi(M_1)}$, hence $(|N'_{\varphi(M_1)}|, M_1) = 1$. Next put $M_2 = M_1|N'_{\varphi(M_1)}|$. Then $1 < |\beta_{\varphi(M_1)}| < |\beta_{\varphi(M_2)}|$ since $6 \le \varphi(M_1) < \varphi(M_2)$. By the same reason as mentioned above for M_1, we see again $(|N'_{\varphi(M_2)}|, M_2) = 1$. Repeating these procedures, we are able to produce an infinite sequence

$$|N'_{2m_1}|, ..., |N'_{2m_k}|, |N'_{\varphi(M_1)}|, ..., |N'_{\varphi(M_n)}|, ...,$$

which consists of relatively prime members in pairs. This is however contrary to the assumption and therefore the assertion follows.

It is obvious that Theorem 6.2 contains the statement that there are infinitely many irregular primes.

Acknowledgment

The author is grateful to the anonymous referee for his/her useful comments on the first version of this paper.

References

[1] T. Agoh, On Bernoulli and Euler numbers, Manuscripta Math. **61** (1988), 1-10.

[2] T. Agoh, On Giuga's conjecture, Manuscripta Math. **87** (1995), 501-510.

[3] W.R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, Ann. of Math. **140** (1994), 1-20.

[4] D. Borwein, J.M. Borwein, P.B. Borwein and R. Girgensohn, Giuga's conjecture on primality, Amer. Math. Monthly, **103** (1996), 40-50.

[5] J. Buhler, R. Crandall, R. Ernvall, T. Metsankyla and M. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, J. Symbolic Comput. **31**(2001), 89–96.

[6] L. Carlitz, Note on irregular primes, Proc. Amer. Math. Soc. **5** (1954), 329-331.

[7] G. Fee and S. Plouffe, An efficient algorithm for the computation of Bernoulli numbers, 2007, http://arxiv.org/pdf/math.NT/0702300.

[8] G. Giuga, Su una presumibile proprietà caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. **83** (1950), 511-528.

[9] K. Iwasawa, *Lectures on p-adic L functions*, Annals of Math. Studies no. 74, Princeton Univ. Press, Princeton, 1972.

[10] K.L. Jensen, Om talteoretiske Egenskaber ved de Bernoulliske Tal, Nyt Tidsskrift f. Math., B, **26** (1915), 73-83.

[11] W. Johnson, p-adic proofs of congruences for the Bernoulli numbers, J. Number Theory, **7** (1975), 251-265.

[12] B.C. Kellner, The equivalence of Giuga's and Agoh's conjectures, 2004, http://arxiv.org/abs/math.NT/0409259.

[13] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Ann. of Math. **39** (1938), 350-360.

[14] Š. Porubský, Voronoï type congruences for Bernoulli numbers, Voronoï's Impact on Modern Science, Book **1**, Proc. Inst. of Math., Nat. Acad. Sci. of Ukraine, 1998, 71-98.

[15] I.Sh. Slavutskii, Staudt and arithmetical properties on Bernoulli numbers, Hist. Sci. **5** (1995), 70-74.

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

[17] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

[18] P.T. Young, Congruences for Bernoulli, Euler, and Stirling Numbers, J. Number Theory, **78**(1999), 204-227,

[19] P.T. Young, Degenerate and n-adic versions of Kummer's congruences for values of Bernoulli polynomials, Discrete Math. **285**(2004), 289-296.