#A12 INTEGERS 16 (2016)

CONGRUENCES RELATED TO THE ANKENY-ARTIN-CHOWLA CONJECTURE

Takashi Agoh[1]
Department of Mathematics, Tokyo University of Science, Noda, Chiba, Japan
agoh_takashi@ma.noda.tus.ac.jp

Received: 11/22/14, Accepted: 1/30/16, Published: 2/29/16

Abstract

Let p be an odd prime with $p \equiv 1 \pmod 4$ and $\varepsilon = (t + u\sqrt{p})/2 > 1$ be the fundamental unit of the real quadratic field $K = \mathbb{Q}(\sqrt{p})$ over the rationals. The Ankeny-Artin-Chowla conjecture asserts that $p \nmid u$, which still remains unsolved. In this paper, we investigate various kinds of congruences equivalent to its negation $p \mid u$ by making use of Dirichlet's class number formula, the products of quadratic residues and non-residues modulo p and a special type of congruence for Bernoulli numbers.

1. Introduction

§ 1.1 Let p be an odd prime with $p \equiv 1 \pmod 4$ and $\mu := (p-1)/2$. Also let h be the class number of the real quadratic field $K := \mathbb{Q}(\sqrt{p})$ over the rationals and $\varepsilon := (t + u\sqrt{p})/2 > 1$ be the fundamental unit of K, where $(x, y) = (t, u)$ is the least positive integer pair satisfying the Pell equation

$$x^2 - py^2 = -4. \tag{1.1}$$

A very important relation between h and ε can be stated by Dirichlet's class number formula

$$h = \frac{\sqrt{p}}{2\log\varepsilon} L(1, \chi) \quad \text{(see, e.g., [25, Chap. 26])}, \tag{1.2}$$

where $L(s, \chi)$ is the L-function attached to the Dirichlet character χ of conductor p, that is, the Legendre symbol in this case.

[1] The author was partially supported by the Ministry of Education, Culture, Sports, Science and Technology in Japan, Grant-in-Aid for Scientific Research (C).

In 1948, the following remarkable congruence was first proved by Kiselev [18], and later independently by Ankeny and Chowla [11]:

$$\frac{hu}{t} \equiv B_\mu \pmod{p}, \tag{1.3}$$

where B_n denotes the nth Bernoulli number defined by the Taylor expansion

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n \quad (|x| < 2\pi). \tag{1.4}$$

In their paper [10] of 1952, Ankeny, Artin and Chowla asked the question whether $p \nmid u$ is always true and this question gradually came to be called the Ankeny-Artin-Chowla (AAC) conjecture. This conjecture remains as yet unsolved and it has attracted a great deal of attention as a possible important property of the fundamental unit of K. Since $h < \sqrt{p}$ (see, e.g., [28, 21]), and so $p \nmid h$, we recognize from (1.3) that the AAC conjecture is actually equivalent to the assertion that $p \nmid B_\mu$ is always true.

According to traditional notation, in what follows we write

$$\varepsilon_n := \varepsilon^n = \left(\frac{t + u\sqrt{p}}{2}\right)^n = \frac{t_n + u_n\sqrt{p}}{2} \quad \text{for} \quad n \geq 1.$$

Then the pair (t_n, u_n) is again a solution of (1.1), and since $2^{n-1}u_n \equiv nt^{n-1}u \pmod{p}$, we may state that $p \nmid u$ is equivalent to $p \nmid u_n$ for any $n \geq 1$ with $p \nmid n$.

It is well-known that if p is a prime of the form $p = n^2 + 1$ with $n > 2$ (i.e., $p = 17, 37, 101, 257, 401, \ldots$), then $\varepsilon = n + \sqrt{n^2+1} = \sqrt{p-1} + \sqrt{p}$ is the fundamental unit of K. Further, if p is a prime of the form $p = n^2 + 4$ with $n \geq 1$ (i.e., $p = 5, 13, 29, 53, 169, 229, \ldots$), then $\varepsilon = (n + \sqrt{n^2+4})/2 = (\sqrt{p-4} + \sqrt{p})/2$ is the fundamental unit of K. These facts tell us that the AAC conjecture is true at least in such special cases.

By numerical computations, van der Poorten et al. verified in [30] that the AAC conjecture holds for all primes $p < 2 \times 10^{11}$ with $p \equiv 1 \pmod{4}$ using a new algorithm for finding an integer $k \geq 1$, $p \nmid k$ for which ε_k (and hence u_k) can be easily computed. Unfortunately, it is still open whether it can happen that $p \nmid u$ for infinitely many primes $p \equiv 1 \pmod{4}$.

On the other hand, it is a fact that there are some counter arguments against this conjecture. For example, based on the heuristic reasoning as mentioned in [33, p. 82], if we view the numerator of B_μ as a random number, then the probability that it is divisible by p is $1/p$. Thus the expected primes $p \leq x$ with $p \equiv 1 \pmod{4}$ and p dividing the numerator of B_μ should be approximately

$$\sum_{\substack{p \leq x \\ p \equiv 1 \ (\mathrm{mod}\ 4)}} \frac{1}{p} \approx \frac{1}{2} \log\log x,$$

which leads to an inference that the AAC conjecture might not be true.

§ 1.2 It is the main purpose of this paper to investigate various kinds of congruences equivalent to $p \mid u$. The paper is organized as follows: In Section 2 we recall the present author's previous results obtained by applying Dirichlet's class number formula and expound them with more detailed analysis and explanations. In Section 3 we first introduce Carlitz's results which used the products of quadratic residues and non-residues modulo p, and we later apply them to derive some variations by means of the Wilson quotient, Fermat quotients and Bernoulli numbers. In Section 4 we concentrate on the study of a special type of congruences for Bernoulli numbers found by Voronoï, Vandiver, Lehmer and other mathematicians, and making use of them, we establish various conditions equivalent to $p \mid B_\mu$ and hence to $p \mid u$.

Here we wish to point out beforehand that this paper includes not only new but also known results, and all the methods we will use are quite elementary without any use of intricate tools.

2. Dirichlet's Class Number Formula and its Application

§ 2.1 Let p be an odd prime with $p \equiv 1 \pmod 4$, $\chi(k) := \left(\frac{k}{p}\right)$ be the Legendre symbol with respect to p and ζ be a primitive pth root of unity. With the help of the quadratic Gauss sum

$$\sum_{k \bmod p} \chi(k)\zeta^{nk} = \chi(n)\sqrt{p},$$

we obtain from (1.2) that

$$\begin{aligned}\log \varepsilon^{2h} &= \sum_{n=1}^{\infty} \frac{1}{n} \left\{ \sum_{k \bmod p} \chi(k)\zeta^{nk} \right\} = \sum_{k=0}^{p-1} \chi(k) \sum_{n=1}^{\infty} \frac{1}{n}\zeta^{nk} \\ &= -\sum_{k=0}^{p-1} \chi(k) \log(1-\zeta^k) = \sum_{k=0}^{p-1} \log(1-\zeta^k)^{-\chi(k)},\end{aligned}$$

which gives

$$\varepsilon_{2h} = \prod_s (1-\zeta^s) \prod_r (1-\zeta^r)^{-1}, \tag{2.1}$$

where r and s are taken over the quadratic residues and non-residues modulo p between 0 and p, respectively. In this section, by applying the expression of ε_{2h} in (2.1), we will deduce some conditions equivalent to $p \mid u$.

§ 2.2 For simplicity, we denote

$$A := \prod_r (1-\zeta^r) \quad \text{and} \quad B := \prod_s (1-\zeta^s).$$

Since $\prod_{j=1}^{p-1}(x-\zeta^j) = x^{p-1}+\cdots+x+1$, putting $x=1$, we have $AB = \prod_{j=1}^{p-1}(1-\zeta^j) = p$. Further, if $p \equiv 1 \pmod 4$, then we see $\left(\frac{k}{p}\right) = \left(\frac{p-k}{p}\right)$ and $(1-\zeta^k)(1-\zeta^{p-k}) = 4\sin^2(\pi k/p) > 0$ for each $k = 1, 2, ..., \mu$, and thus $A, B > 0$.

The magnitude relation between A and B can be determined as follows:

Lemma 2.1. *Let p be an odd prime with $p \equiv 1 \pmod 4$. Then we have*

$$B \geq \sqrt{p}\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^h > \sqrt{p}\left(\frac{\sqrt{p}-\sqrt{p-4}}{2}\right)^h \geq A > 0. \tag{2.2}$$

Proof. Since t and u are the least positive integers satisfying (1.1), we see that $u \geq 1$ and $t \geq \sqrt{p-4}$, and so $\varepsilon \geq \frac{1}{2}\left(\sqrt{p}+\sqrt{p-4}\right)$. Based on this fact, we get

$$\varepsilon_h = \sqrt{\frac{B}{A}} = \frac{B}{\sqrt{p}} = \frac{\sqrt{p}}{A} \geq \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^h = \left(\frac{2}{\sqrt{p}-\sqrt{p-4}}\right)^h > 0,$$

which proves (2.2). □

It is easily seen that there exist unique integers a, b and c such that

$$\begin{aligned} A &= a + b\sum_r \zeta^r + c\sum_s \zeta^s; \\ B &= a + b\sum_s \zeta^s + c\sum_r \zeta^r, \end{aligned} \tag{2.3}$$

where the sums $\sum_r$ and $\sum_s$ run over the quadratic residues r and non-residues s modulo p between 0 and p, respectively. Throughout this paper, we will use the same sum notations unless otherwise noted.

Using the well-known identities

$$\sum_r \zeta^r + \sum_s \zeta^s = -1 \quad \text{and} \quad \sum_r \zeta^r - \sum_s \zeta^s = \sqrt{p}, \tag{2.4}$$

we obtain from (2.3) that

$$A + B = 2a - (b+c) = -(b+c)p \quad \text{and} \quad A - B = (b-c)\sqrt{p}. \tag{2.5}$$

Since $A + B > 0$ and $A - B < 0$ by Lemma 2.1, we see $a > 0$ and $b \pm c < 0$. Also, it is clear that basic relations between a, b and c are given by

$$\begin{aligned} a + \mu(b+c) &= 0; \\ (b-c)^2 + 4 &= p(b+c)^2, \end{aligned} \tag{2.6}$$

which are easily shown by using (2.5).

On the other hand, we can obtain from (2.1) and (2.5) that

$$\varepsilon_h = \frac{B}{\sqrt{p}} = \frac{1}{2}\left(-\frac{A-B}{\sqrt{p}} + \frac{A+B}{p}\sqrt{p}\right) = \frac{-(b-c)-(b+c)\sqrt{p}}{2}. \tag{2.7}$$

Since $\mu \mid a$, set $a' := a/\mu$. Using (2.6), if we rewrite (2.7) in terms of a or a', then

$$\varepsilon_h = \frac{1}{p-1}\left(\sqrt{pa^2-(p-1)^2} + a\sqrt{p}\right) = \frac{\sqrt{pa'^2-4}+a'\sqrt{p}}{2}. \tag{2.8}$$

Therefore, we have

$$\begin{aligned} t_h &= -(b-c) = \frac{1}{\mu}\sqrt{pa^2-(p-1)^2} = \sqrt{pa'^2-4}\,; \\ u_h &= -(b+c) = \frac{1}{\mu}a = a'. \end{aligned} \tag{2.9}$$

Here note that $pa^2-(p-1)^2$, and so pa'^2-4, are perfect squares. Also, rewriting the second identity in (2.6) as $(p-1)b^2+2(p+1)bc+(p-1)c^2-4=0$, if we solve this identity as an equation for b (resp. c) in terms of c (resp. b), then we notice that both pb^2+p-1 and pc^2+p-1 must be perfect squares, because b and c are integers.

In addition, since $t_h \equiv t^h/2^h \pmod{p}$ and $u_h \equiv ht^{h-1}u/2^h \pmod{p}$, we can deduce the congruence

$$\frac{u_h}{t_h} = \frac{b+c}{b-c} = \frac{a'}{\sqrt{pa'^2-4}} \equiv \frac{hu}{t} \equiv B_\mu \pmod{p}. \tag{2.10}$$

With these preparations, we are able to state the following theorem already mentioned in [1, Theorem 3]:

Theorem 2.2. *If* $p \equiv 1 \pmod{4}$*, then* $p \mid u$ *is equivalent to each of*

(i) $a \equiv 0 \pmod{p}$; (ii) $b+c \equiv 0 \pmod{p}$; (iii) $bc \equiv 1 \pmod{p^2}$.

Proof. Since $p \mid u$ is equivalent to $p \mid u_h$, we see from (2.9) that each of (i) and (ii) is equivalent to $p \mid u$. It is also obvious that (ii) is equivalent to (iii) if we consider the second identity in (2.6), rewritten as $(1-p)(b+c)^2 = 4(bc-1)$. □

§ 2.3 As was already mentioned in [1, 7], we may write A as $A = \prod_{k=1}^{\mu}(1-\zeta^{k^2})$; therefore the integer a in (2.3) can be represented by

$$a = \mu a' = 1 + \sum_{k=1}^{\mu}(-1)^k N_k,$$

where N_k is the number such that

$$N_k := \mathrm{Card}\Big\{(x_1,...,x_k)\,\Big|\,\sum_{i=1}^{k} x_i^2 \equiv 0 \pmod{p},\ 1 \leq x_1 < \cdots < x_k \leq \mu\Big\}.$$

For example, if $p = 13$, then the k-tuples $(x_1,...,x_k)$ satisfying $\sum_{i=1}^{k} x_i^2 \equiv 0 \pmod{13}$ and $1 \leq x_1 < \cdots < x_k \leq 6$ are given as follows: $(1,5),(2,3),(4,6)$ for $k = 2$; $(1,3,4),(2,5,6)$ for $k = 3$; $(1,2,3,5),(1,4,5,6),(2,3,4,6)$ for $k = 4$; $(1,2,3,4,5,6)$ for $k = 6$. Thus $a = 1 + (3 - 2 + 3 + 1) = 6$, and so $a' = 6/6 = 1$.

As a matter of fact, it is not so easy to compute the above N_k. Some recursive methods of obtaining N_k have been found by Le [20] and Iyanaga [17]. An explicit formula for N_k was completed by Shoji and the present author in [7] by means of the number of certain quadratic hyper-surfaces in the vector space $\mathbb{F}_p^k$ over the finite field $\mathbb{F}_p$ with p elements, which is however rather complicated to restate here.

If we represent b and c in terms of a (or a'), then we get from (2.9) that

$$b = -\frac{1}{p-1}\left(\sqrt{pa^2-(p-1)^2}+a\right) = -\frac{1}{2}\left(\sqrt{pa'^2-4}+a'\right);$$
$$c = \frac{1}{p-1}\left(\sqrt{pa^2-(p-1)^2}-a\right) = \frac{1}{2}\left(\sqrt{pa'^2-4}-a'\right).$$

Since $a > 0$, we see that $b < 0$. Also, by (2.5) and Lemma 2.1, if $p > 5$, then

$$A + B = 2a - (b + c) = \frac{2ap}{p-1} > \frac{p+\sqrt{p^2-4p}}{2} > \frac{2p}{\sqrt{p-1}} > 0.$$

Thus $a > \sqrt{p-1}$, which shows that $\sqrt{pa^2-(p-1)^2} > a$ and so $c > 0$ for $p > 5$. When $p = 5$, we have $a = 2$, $b = -1$ and $c = 0$ by direct calculation.

If a was obtained in some way, then it is possible to deduce b and c immediately using the above formulas. However, we do not have a good idea at this moment how to compute a itself in an easy way based only on the definition in (2.3) without any information of ε and h.

§ 2.4 Next, we assume that p is an odd prime with $p \equiv 5 \pmod{8}$. Then it is clear that there exist unique integers α, β and γ such that

$$\begin{aligned} A' &:= \prod_r (1+\zeta^r) = \alpha + \beta\sum_r \zeta^r + \gamma\sum_s \zeta^s;\\ B' &:= \prod_s (1+\zeta^s) = \alpha + \beta\sum_s \zeta^s + \gamma\sum_r \zeta^r. \end{aligned} \tag{2.11}$$

These integers α, β and γ are obviously positive and they satisfy the conditions

$$\begin{aligned} \alpha + \mu(\beta+\gamma) &= 2^\mu;\\ \big(2^{\mu+1} - p(\beta+\gamma)\big)^2 - 4 &= p(\beta-\gamma)^2. \end{aligned} \tag{2.12}$$

Similar to Lemma 2.1, the magnitude relation between A' and B' is determined as follows:

Lemma 2.3. *If $p \equiv 5 \pmod 8$, then*

$$A' \geq \left(\frac{p-2+\sqrt{p^2-4p}}{2}\right)^h > \left(\frac{p-2-\sqrt{p^2-4p}}{2}\right)^h \geq B' > 0. \tag{2.13}$$

Proof. Since $(1+\zeta^k)(1+\zeta^{p-k}) = 4\cos^2(\pi k/p) > 0$ for $k = 1, 2, ..., \mu$, it is obvious that $A', B' > 0$. If $p \equiv 5 \pmod 8$, then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = -1$, thus $\left(\frac{2s}{p}\right) = 1$ and $\left(\frac{2r}{p}\right) = -1$. So it follows that $A = BB'$ and $B = AA'$. Also, taking $x = 1$ in the identity $(x^p+1)/(x+1) = \prod_{j=1}^{p-1}(x+\zeta^j)$, we have $A'B' = 1$. Since $\varepsilon \geq \frac{1}{2}\left(\sqrt{p}+\sqrt{p-4}\right)$ as stated in the proof of Lemma 2.1, we obtain

$$\begin{aligned}\varepsilon_{2h} = \frac{B}{A} = A' = \frac{1}{B'} \geq \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^{2h} &= \left(\frac{p-2+\sqrt{p^2-4p}}{2}\right)^h \\ &= \left(\frac{2}{p-2-\sqrt{p^2-4p}}\right)^h > 0,\end{aligned}$$

which proves (2.13). □

Using (2.4), (2.12) and (2.13), we can deduce from (2.11) that

$$\begin{aligned}&A' + B' = 2\alpha - (\beta+\gamma) = 2^{\mu+1} - (\beta+\gamma)p > 0;\\ &A' - B' = (\beta-\gamma)\sqrt{p} > 0.\end{aligned}$$

Based on these identities, it is shown that if $p \equiv 5 \pmod 8$, then

$$\varepsilon_{2h} = A' = \frac{(A'+B')+(A'-B')}{2} = \frac{2^{\mu+1}-(\beta+\gamma)p+(\beta-\gamma)\sqrt{p}}{2}.$$

Therefore, from (2.12) we have

$$\begin{aligned}t_{2h} &= 2^{\mu+1} - (\beta+\gamma)p = \frac{1}{\mu}(p\alpha - 2^\mu);\\ u_{2h} &= \beta - \gamma = \frac{1}{\mu\sqrt{p}}\sqrt{(p\alpha-2^\mu)^2-(p-1)^2} = \frac{1}{\mu}\sqrt{M_p(\alpha)},\end{aligned} \tag{2.14}$$

where $M_p(\alpha) := p(\alpha^2-1) - 2\left(2^\mu\alpha - 1\right) + q_p(2)$ and $q_p(2) := (2^{p-1}-1)/p$ is the Fermat quotient of p with base 2. Needless to say, $M_p(\alpha)$ is a perfect square.

With the above observations, we establish the following theorem which is already mentioned in [1, Theorem 4]:

Theorem 2.4. *If $p \equiv 5 \pmod 8$, then $p \mid u$ is equivalent to each of*

$$\text{(i)}\quad \alpha \equiv -1 - \frac{1}{2}q_p(2) \pmod p; \qquad \text{(ii)}\quad \beta \equiv \gamma \equiv -\frac{1}{2}q_p(2) \pmod p;$$
$$\text{(iii)}\quad \beta + \gamma \equiv -q_p(2) \pmod p.$$

Proof. It is obvious that (ii) implies (iii). From (2.14), we see that $p \mid u$ is equivalent to $p \mid u_{2h}$, and hence to $\beta \equiv \gamma \pmod p$. If $\beta \equiv \gamma \pmod p$, then, by using the second identity in (2.12) we have

$$\left(2^{\mu+1} - p(\beta+\gamma)\right)^2 - 4 \equiv 4\left((2^{p-1}-1) - 2^{\mu+1}p\beta\right) \equiv 0 \pmod{p^2},$$

which gives $\beta \equiv -q_p(2)/2 \pmod p$, and so $\gamma \equiv -q_p(2)/2 \pmod p$, because $\left(\frac{2}{p}\right) \equiv 2^\mu \equiv -1 \pmod p$ holds whenever $p \equiv 5 \pmod 8$. Thus, we recognize that $p \mid u$ is equivalent to (ii). Also, from the first identity in (2.12), it is clear that (i) implies (iii), and vice versa. Using again the second identity in (2.12), we observe that (iii) yields $\beta \equiv \gamma \pmod p$. This completes the proof of the theorem. □

§ 2.5 Similar to the case of a, it is possible to represent α by means of N_k defined in Subsection 2.3. Indeed, by writing A' as $A' = \prod_{k=1}^{\mu}(1+\zeta^{k^2})$ we see that

$$\alpha = 1 + \sum_{k=1}^{\mu} N_k.$$

If α was given in some way, then β and γ can be obtained by using the following formulas derived from (2.14):

$$\beta = \frac{1}{p-1}\left(2^\mu - \alpha + \sqrt{M_p(\alpha)}\right); \quad \gamma = \frac{1}{p-1}\left(2^\mu - \alpha - \sqrt{M_p(\alpha)}\right). \tag{2.15}$$

For example, if $p = 13$, then $N_1 = 0, N_2 = 3, N_3 = 2, N_4 = 3, N_5 = 0$ and $N_6 = 1$ as was seen in Subsection 2.3; thus we have $\alpha = 1 + (3+2+3+1) = 10$. Then $M_{13}(10) = 13(10^2-1) - 2\left(2^6 \cdot 10 - 1\right) + q_{13}(2) = 324$, and hence $\sqrt{M_{13}(10)} = 18$. By using this value we get $\beta = (2^6 - 10 + 18)/12 = 6$ and $\gamma = (2^6 - 10 - 18)/12 = 3$.

Incidentally, if $p \equiv 5 \pmod 8$, then $2^\mu \equiv -1 \pmod p$, and thus we can deduce from (2.14) and (2.15) that

$$\frac{u_{2h}}{t_{2h}} = \frac{\beta - \gamma}{2^{\mu+1} - (\beta+\gamma)p} \equiv -\frac{\beta-\gamma}{2} \equiv \sqrt{M_p(\alpha)} \equiv 2B_\mu \pmod p.$$

Making use of this congruence, we see at once that $p \mid u$ is equivalent to each of

$$\text{(i)}\quad p \mid B_\mu; \quad \text{(ii)}\quad p \mid \beta - \gamma; \quad \text{(iii)}\quad p^2 \mid M_p(\alpha).$$

3. Products of Quadratic Residues and Non-residues

§ 3.1 In this subsection, we will discuss some congruences equivalent to $p \mid u$ which are related to the individual products of quadratic residues and non-residues modulo p, while mainly referring to results of Carlitz.

In what follows, we denote by $R := \prod_r r$ and $S := \prod_s s$ the products of the quadratic residues r and non-residues s modulo p between 0 and p, respectively.

If $p \equiv 1 \pmod 4$, then $\left(\frac{k}{p}\right) = \left(\frac{p-k}{p}\right)$ $(k = 1, 2, ..., \mu)$, hence by using Wilson's theorem (i.e., $(p-1)! \equiv -1 \pmod p$) we get

$$R \equiv (\mu!)^2 \equiv (-1)^{\mu}(p-1)! \equiv -1 \pmod p;$$
$$S = \frac{(p-1)!}{R} \equiv (-1)^{\mu} \equiv 1 \pmod p.$$

So there exist the integers $U_p > 0$ and $V_P < 0$ such that

$$R + 1 = pU_p \quad \text{and} \quad S - 1 = -pV_p. \tag{3.1}$$

The following remarkable congruence was first announced by Ankeny, Artin and Chowla in [9], and later proved by Carlitz in [14]:

$$\frac{u_{2h}}{t_{2h}} \equiv \frac{2hu}{t} \equiv \frac{R+S}{p} \pmod p. \tag{3.2}$$

Since $\varepsilon_{2h} = \varepsilon_h^2$, we obtain from (2.9) and (2.10) that

$$\frac{u_{2h}}{t_{2h}} = \frac{2t_h u_h}{t_h^2 + pu_h^2} = \frac{2(b^2 - c^2)}{(b-c)^2 + p(b+c)^2} \equiv \frac{2(b+c)}{b-c} \equiv 2B_{\mu} \pmod p.$$

Therefore, by using (3.1) and (3.2) we have

$$\frac{R+S}{p} = U_p - V_p \equiv 2B_{\mu} \pmod p. \tag{3.3}$$

Consequently, as Carlitz already mentioned, it can be shown from (3.3) that $p \mid u$ is equivalent to each of

$$\text{(i)}\ \ p \mid B_{\mu}; \quad \text{(ii)}\ \ p^2 \mid R + S; \quad \text{(iii)}\ \ p \mid U_p - V_p. \tag{3.4}$$

Let $W_p := ((p-1)! + 1)/p$ be the Wilson quotient for an odd prime p. We now recall the following classical formulas supplying some relations between W_p and specific Bernoulli numbers:

$$\begin{aligned} &W_p \equiv B_{p-1} + \frac{1}{p} - 1 \pmod p \quad \text{(Beeger [12], Lerch [24])}; \\ &W_p \equiv B_{2(p-1)} - B_{p-1} \pmod p \quad \text{(E. Lehmer [22])}. \end{aligned} \tag{3.5}$$

Here note that the right-hand sides of these congruences are p-integral by the von Staudt-Clausen Theorem. For the proof of (3.5), see, e.g., [2, Proposition 3.12].

As is easily seen, if $p \equiv 1 \pmod 4$, then it follows that

$$(p-1)! = RS = (-1 + pU_P)\,(1 - pV_p) \equiv -1 + p(U_p + V_p) \pmod{p^2},$$

and so, dividing by p we get $W_p \equiv U_p + V_p \pmod p$. Combining this with (3.3),

$$W_p \equiv 2\,(U_p - B_\mu) \equiv 2\,(V_p + B_\mu) \pmod p. \tag{3.6}$$

Theorem 3.1. *If $p \equiv 1 \pmod 4$, then $p \mid u$ is equivalent to each of*

$$\begin{aligned} &\text{(i)} \quad W_p \equiv 2U_p \equiv 2V_p \pmod p;\\ &\text{(ii)} \quad B_{p-1} + \frac{1}{p} \equiv 2U_p + 1 \equiv 2V_p + 1 \pmod p;\\ &\text{(iii)} \quad B_{2(p-1)} - B_{p-1} \equiv 2U_p \equiv 2V_p \pmod p. \end{aligned}$$

Proof. In view of (3.3) and (3.6), it is clear that $p \mid B_\mu$ is equivalent to (i). Also, the conditions (ii) and (iii) are derived by applying (i) and (3.5). □

§ 3.2 If one of U_p and V_p was known, then the other one can be given from the congruence $W_p \equiv U_p + V_p \pmod p$ mentioned above. It may be somewhat crude, but we want to introduce below one of the methods of obtaining U_p and V_p modulo p without the use of any quadratic residues and non-residues.

If r is a quadratic residue modulo p, then there exists a unique integer j, $1 \le j \le \mu$, such that $r \equiv j^2 \pmod p$, and so $r = j^2 - \lfloor j^2/p \rfloor p$. Therefore, we have

$$R = \prod_r r = \prod_{j=1}^{\mu} \Big(j^2 - \Big\lfloor \frac{j^2}{p} \Big\rfloor p \Big) \equiv (\mu!)^2 \left(1 - p \sum_{j=1}^{\mu} \frac{1}{j^2} \Big\lfloor \frac{j^2}{p} \Big\rfloor \right) \pmod{p^2}.$$

Since $(p-1)! \equiv (-1)^\mu \,(\mu!)^2 \equiv -1 \pmod p$ by Wilson's theorem, we have $(\mu!)^2 \equiv -1 \pmod p$, and hence

$$U_p = \frac{R+1}{p} \equiv \frac{(\mu!)^2 + 1}{p} + \sum_{j=\lfloor\sqrt{p}\rfloor+1}^{\mu} \frac{1}{j^2} \Big\lfloor \frac{j^2}{p} \Big\rfloor \pmod p.$$

Also, using the congruence $(p-1)! \equiv (\mu!)^2(1 - pH_\mu) \pmod{p^2}$, it follows that

$$W_p \equiv \frac{(\mu!)^2 + 1}{p} - (\mu!)^2 H_\mu \pmod p,$$

where $H_k := 1 + 1/2 + \cdots + 1/k$ is the kth harmonic number. As a result, we have

$$V_p \equiv W_p - U_p \equiv -(\mu!)^2 H_\mu - \sum_{j=\lfloor\sqrt{p}\rfloor+1}^{\mu} \frac{1}{j^2} \Big\lfloor \frac{j^2}{p} \Big\rfloor \pmod p.$$

§ 3.3 For a positive integer n with $p \nmid n$, let $q_p(n) := (n^{p-1}-1)/p$ be the Fermat quotient of p with base n. We first present the well-known logarithmic property of Fermat quotients, which can be easily shown by using Fermat's little theorem.

Lemma 3.2. *Let k and m be positive integers prime to p. Then it follows that $q_p(km) \equiv q_p(k) + q_p(m) \pmod{p}$.*

Theorem 3.3. *If $p \equiv 1 \pmod 4$, then $p \mid u$ is equivalent to each of*

$$\text{(i)} \quad \sum_r q_p(r) \equiv \sum_s q_p(s) \pmod{p};$$

$$\text{(ii)} \quad \sum_{0<r<p/2} \left(2q_p(r) + \frac{1}{r}\right) \equiv \sum_{0<s<p/2} \left(2q_p(s) + \frac{1}{s}\right) \pmod{p}.$$

Proof. Since $R = -1 + pU_p$ and $S = 1 - pV_p$, we have $(R+S)/p = U_p - V_p$, as already mentioned in Subsection 3.1. On the other hand, from the definition of the Fermat quotient we have

$$q_p(R) = \frac{1}{p}\left((-1+pU_p)^{p-1} - 1\right) \equiv U_p \pmod{p};$$
$$q_p(S) = \frac{1}{p}\left((1-pV_p)^{p-1} - 1\right) \equiv V_p \pmod{p}.$$

Therefore, by making use of Lemma 3.2 we obtain from (3.3) that

$$\begin{aligned} \frac{R+S}{p} &= U_p - V_p \equiv q_p(R) - q_p(S) \\ &\equiv \sum_r q_p(r) - \sum_s q_p(s) \equiv 2B_\mu \pmod{p}, \end{aligned} \tag{3.7}$$

which proves that $p \mid B_\mu$ is equivalent to (i). Next, noting that

$$\begin{aligned} q_p(p-m) = \frac{(p-m)^{p-1}-1}{p} &\equiv q_p(m) - (p-1)m^{p-2} \\ &\equiv q_p(m) + \frac{1}{m} \pmod{p} \end{aligned}$$

and $\left(\frac{m}{p}\right) = \left(\frac{p-m}{p}\right)$ for each $m = 1, 2, ..., \mu$, we get from (3.7) that

$$\begin{aligned} \sum_r q_p(r) - \sum_s q_p(s) &\equiv \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) q_p(m) \\ &\equiv \sum_{m=1}^{\mu} \left(\left(\frac{m}{p}\right) q_p(m) + \left(\frac{p-m}{p}\right) q_p(p-m)\right) \\ &\equiv \sum_{m=1}^{\mu} \left(\frac{m}{p}\right)\left(2q_p(m) + \frac{1}{m}\right) \equiv 2B_\mu \pmod{p}, \end{aligned}$$

which shows that (i) is equivalent to (ii). □

In Section 4 we will give a direct proof of (3.7) and hence of Proposition 3.3 (i), based on a certain congruence for Bernoulli numbers, without the use of (3.3).

Theorem 3.4. *Let p be an odd prime with $p \equiv 1 \pmod 4$ and s' be any fixed quadratic non-residue modulo p. Then $p \mid u$ is equivalent to*

$$q_p(s') \equiv \frac{2}{s'} \sum_{p/s'<r<p} \frac{1}{r} \left\lfloor \frac{s'r}{p} \right\rfloor \pmod p. \tag{3.8}$$

Proof. Since $\left(\frac{s'}{p}\right) \equiv s'^{\mu} \equiv -1 \pmod p$, we have

$$U_p - V_p \equiv -s'^{\mu} \frac{R+S}{p} \equiv -\frac{1}{p} \left(\prod_r (s'r) + s'^{\mu} S \right) \pmod p. \tag{3.9}$$

For a quadratic residue r, let c_r be the least positive residue of $s'r$ modulo p. Since $s'r = \lfloor s'r/p \rfloor p + c_r \equiv c_r \pmod p$, we have $\left(\frac{c_r}{p}\right) = \left(\frac{s'}{p}\right)\left(\frac{r}{p}\right) = -1$. Further, for quadratic residues r_1 and r_2 modulo p, we see that $r_1 \neq r_2$ if and only if $c_{r_1} \neq c_{r_2}$, and so $\prod_r c_r = S$ follows. Based on this fact, we can obtain the congruence

$$\prod_r (s'r) = \prod_r \left(c_r + \left\lfloor \frac{s'r}{p} \right\rfloor p \right) \equiv S \left(1 + p \sum_r \frac{1}{c_r} \left\lfloor \frac{s'r}{p} \right\rfloor \right) \pmod{p^2}.$$

Thus, using $(s'^{\mu}+1)/p \equiv -q_p(s')/2 \pmod p$ the right-hand side of (3.9) becomes

$$\begin{aligned} -\frac{1}{p} \left(\prod_r (s'r) + s'^{\mu} S \right) &\equiv -S \left(\frac{s'^{\mu}+1}{p} + \sum_r \frac{1}{c_r} \left\lfloor \frac{s'r}{p} \right\rfloor \right) \\ &\equiv S \left(\frac{1}{2} q_p(s') - \sum_r \frac{1}{c_r} \left\lfloor \frac{s'r}{p} \right\rfloor \right) \pmod p. \end{aligned}$$

If $s'r < p$, then $\lfloor s'r/p \rfloor = 0$, so we get from (3.9) that, exchanging c_r for $s'r$,

$$U_p - V_p \equiv S \left(\frac{1}{2} q_p(s') - \sum_{p/s'<r<p} \frac{1}{s'r} \left\lfloor \frac{s'r}{p} \right\rfloor \right) \pmod p,$$

which shows that (3.8) is equivalent to $p \mid U_p - V_p$ and hence to $p \mid u$ by (3.4), because p does not divide S. This completes the proof of the theorem. □

4. Application of Bernoulli Number Congruences

§ 4.1 In this section, we prepare special type congruences for Bernoulli numbers expressing exactly B_k/k ($k > 0$, an even), and by making use of them we will derive various kinds of conditions equivalent to $p \mid B_{\mu}$, and hence to $p \mid u$.

In what follows, we denote by g a primitive root modulo p and by g_i the least positive residue of g^i modulo p, i.e., $g^i \equiv g_i \pmod{p}$, $1 \leq g_i \leq p-1$.

Let $S_k(n) := 1^k + 2^k + \cdots + (n-1)^k$ for integers $k \geq 1$ and $n \geq 2$. First of all, we present an important consequence of the well-known Euler-Maclaurin summation formula expressing $S_k(n)$ by means of Bernoulli numbers. That is, if $k \geq 1$ and $n \geq 2$, then

$$S_k(n) = \sum_{i=0}^{k} \frac{1}{i+1} \binom{k}{i} n^{i+1} B_{k-i}. \tag{4.1}$$

This formula itself can be derived by expanding both sides of $(x/(e^x-1))(e^{nx}-1) = x\sum_{j=0}^{n-1} e^{jx}$ into the Maclaurin power series and then comparing coefficients of the powers of x. Here note that $\frac{1}{i+1}\binom{k}{i} = \frac{1}{k+1}\binom{k+1}{i+1}$ for each $i \geq 0$.

Using the von Staudt-Clausen theorem and (4.1) with $n = p$, we can prove the following proposition (see [2, 29], for instance):

Proposition 4.1. *If p is an odd prime, then*

$$S_k(p) \equiv \begin{cases} -1 \pmod{p} & \textit{if } \ p-1 \mid k; \\ \ \ 0 \pmod{p} & \textit{otherwise.} \end{cases} \tag{4.2}$$

In particular, if $k \geq 2$ is even and $p - 1 \nmid k$, then

$$S_k(p) \equiv pB_k \pmod{p^2}. \tag{4.3}$$

By making use of (4.3) we may state the following theorem:

Theorem 4.2. *If $p \equiv 1 \pmod 4$, then $p \mid u$ is equivalent to*

$$\frac{1}{p}\sum_{i=0}^{p-2} \frac{(-g)^i}{g_i} \equiv -\frac{1}{2} q_p(g) \pmod{p}. \tag{4.4}$$

Proof. First we note that

$$\begin{aligned} g^{\mu(p-1)} - 1 = (g^{p-1} - 1 + 1)^{\mu} - 1 &= \sum_{j=0}^{\mu} \binom{\mu}{j} (g^{p-1} - 1)^j - 1 \\ &\equiv \mu(g^{p-1} - 1) \equiv -\frac{1}{2}(g^{p-1} - 1) \pmod{p^2}. \end{aligned}$$

Dividing this by $g^{\mu} - 1$, we have $(g^{\mu(p-1)} - 1)/(g^{\mu} - 1) \equiv (g^{p-1} - 1)/4 \pmod{p^2}$, because $g^{\mu} \equiv -1 \pmod{p}$ holds for a primitive root g modulo p. Also, since

$g_i = g^i - \lfloor g^i/p \rfloor p$, by taking $k = \mu$ in (4.3) we have

$$\begin{aligned} S_\mu(p) &= \sum_{i=0}^{p-2} g_i^\mu = \sum_{i=0}^{p-2} \left(g^i - \left\lfloor \frac{g^i}{p} \right\rfloor p \right)^\mu \equiv \sum_{i=0}^{p-2} \left(g^{i\mu} - \mu g^{i(\mu-1)} \left\lfloor \frac{g^i}{p} \right\rfloor p \right) \\ &\equiv \frac{g^{\mu(p-1)} - 1}{g^\mu - 1} + \frac{p}{2} \sum_{i=0}^{p-2} g^{i(\mu-1)} \left\lfloor \frac{g^i}{p} \right\rfloor \equiv \frac{1}{4}(g^{p-1} - 1) + \frac{1}{2} \sum_{i=0}^{p-2} \frac{(-1)^i}{g_i}(g^i - g_i) \\ &\equiv \frac{p}{4} q_p(g) + \frac{1}{2} \sum_{i=0}^{p-2} \frac{(-g)^i}{g_i} \equiv pB_\mu \pmod{p^2}, \end{aligned}$$

which proves, after dividing by p, that (4.4) is equivalent to $p \mid B_\mu$. □

Proposition 4.3. *Let k be a positive integer such that $p - 1 \nmid k$. Then*

$$\sum_{m=1}^{p-1} m^k q_p(m) \equiv -\frac{B_k}{k} \pmod{p}. \tag{4.5}$$

Proof. The Kummer congruence asserts that if $p - 1 \nmid k$, then

$$\frac{B_{k+p-1}}{k+p-1} \equiv \frac{B_k}{k} \pmod{p},$$

which yields $B_{k+p-1} \equiv ((k-1)/k)\, B_k \pmod{p}$. Therefore, by making use of (4.3) in Proposition 4.1 we obtain

$$\begin{aligned} \sum_{m=1}^{p-1} m^k q_p(m) &= \sum_{m=1}^{p-1} \frac{m^k(m^{p-1} - 1)}{p} \equiv \frac{1}{p}\left(S_{k+p-1}(p) - S_k(p)\right) \\ &\equiv B_{k+p-1} - B_k \equiv \frac{k-1}{k} B_k - B_k \equiv -\frac{B_k}{k} \pmod{p}, \end{aligned}$$

which proves that (4.5) follows. □

In particular, considering the special case where $k = \mu$ in (4.5), we have

$$\sum_{m=1}^{p-1} m^\mu q_p(m) \equiv \sum_{m=1}^{p-1} \left(\frac{m}{p} \right) q_p(m) \equiv \sum_r q_p(r) - \sum_s q_p(s) \equiv -\frac{B_\mu}{\mu} \pmod{p},$$

which gives another proof of Theorem 3.3 (i) without the use of (3.3).

§ 4.2 For the next discussion, we introduce Voronoï's congruences using a primitive root g modulo p, and by applying these we derive some conditions equivalent to $p \mid \mu$.

Proposition 4.4. *Let p be an odd prime, $k \geq 2$ be an even integer with $p-1 \nmid k$ and a be a positive integer with $p \nmid a$. Then we have*

$$\text{(i)} \quad (a^k-1)\frac{B_k}{k} \equiv \sum_{i=0}^{p-2}(ag_i)^{k-1}\left\lfloor \frac{ag_i}{p} \right\rfloor \pmod{p};$$

$$\text{(ii)} \quad (a^k-1)\frac{B_k}{k} \equiv 2\sum_{j=0}^{\mu-1}(ag_j)^{k-1}\left\lfloor \frac{ag_j}{p} \right\rfloor + \frac{2(a-1)a^{k-1}}{g^{k-1}-1} \pmod{p}.$$

The proof of (i) can be found in many textbooks (for instance, see [29]), so it may be unnecessary to reprove it. However, in order to make a basis of (ii) clear, we would like to give a full proof of this proposition.

Proof. For a fixed integer a, let c_i be the least positive residue of ag_i modulo p, i.e., c_i is the integer such that $ag_i = \lfloor ag_i/p \rfloor p + c_i$, $1 \leq c_i \leq p-1$. Then, it is shown by direct calculation that

$$\sum_{i=0}^{p-2}(ag_i)^k = \sum_{i=0}^{p-2}\left(\left\lfloor \frac{ag_i}{p} \right\rfloor p + c_i\right)^k \equiv \sum_{i=0}^{p-2}\left(k\left\lfloor \frac{ag_i}{p} \right\rfloor pc_i^{k-1} + c_i^k\right) \pmod{p^2}.$$

Hence, the fact that $\{g_i \mid i = 0, 1, ..., p-2\} = \{c_i \mid i = 0, 1, ..., p-2\}$ leads to

$$(a^k-1)S_k(p) \equiv kp\sum_{i=0}^{p-2}c_i^{k-1}\left\lfloor \frac{ag_i}{p} \right\rfloor \pmod{p^2}.$$

Dividing this by p and exchanging c_i for ag_i, we see from (4.3) that (i) follows. On the other hand, since $g_i + g_{\mu+i} = c_i + c_{\mu+i} = p$, the identity

$$a(g_i + g_{\mu+i}) = \left(\left\lfloor \frac{ag_i}{p} \right\rfloor + \left\lfloor \frac{ag_{\mu+i}}{p} \right\rfloor\right)p + c_i + c_{\mu+i}$$

gives, dividing by p,

$$\left\lfloor \frac{ag_i}{p} \right\rfloor + \left\lfloor \frac{ag_{\mu+i}}{p} \right\rfloor = a-1.$$

Also, since $g^{(k-1)\mu} \equiv (-1)^{k-1} \equiv -1 \pmod{p}$ for an even integer k, we have

$$\sum_{j=0}^{\mu-1}(ag_j)^{k-1} \equiv a^{k-1}\sum_{j=0}^{\mu-1}g^{(k-1)j} \equiv a^{k-1}\frac{g^{(k-1)\mu}-1}{g^{k-1}-1} \equiv -\frac{2a^{k-1}}{g^{k-1}-1} \pmod{p}.$$

Making use of this congruence, the sum on the right-hand side of congruence (i) above can be written as

$$\begin{aligned}\sum_{i=0}^{p-2}(ag_i)^{k-1}\left\lfloor\frac{ag_i}{p}\right\rfloor &= \sum_{j=0}^{\mu-1}\left((ag_j)^{k-1}\left\lfloor\frac{ag_j}{p}\right\rfloor + (ag_{\mu+j})^{k-1}\left\lfloor\frac{ag_{\mu+j}}{p}\right\rfloor\right)\\
&= \sum_{j=0}^{\mu-1}\left((ag_j)^{k-1}\left\lfloor\frac{ag_j}{p}\right\rfloor + a^{k-1}(p-g_j)^{k-1}\left\lfloor\frac{ag_{\mu+j}}{p}\right\rfloor\right)\\
&\equiv \sum_{j=0}^{\mu-1}\left((ag_j)^{k-1}\left\lfloor\frac{ag_j}{p}\right\rfloor + (-ag_j)^{k-1}\left(a-1-\left\lfloor\frac{ag_j}{p}\right\rfloor\right)\right)\\
&\equiv \sum_{j=0}^{\mu-1}(ag_j)^{k-1}\left(2\left\lfloor\frac{ag_j}{p}\right\rfloor-(a-1)\right)\\
&\equiv 2\sum_{j=0}^{\mu-1}(ag_j)^{k-1}\left\lfloor\frac{ag_j}{p}\right\rfloor + \frac{2(a-1)a^{k-1}}{g^{k-1}-1} \pmod{p},\end{aligned}$$

and this shows that (ii) follows. □

Incidentally, we would like to mention that Voronoï's congruence introduced in Proposition 4.4 (i) can be generalized for a modulus p^{e+1} $(e \geq 0)$ and it is used to prove the generalized Kummer congruence $(1-p^{m-1})B_m/m \equiv (1-p^{n-1})B_n/n \pmod{p^{e+1}}$ deeply concerned with the construction of p-adic L-function, where m and n are positive integers such that $p-1 \nmid m$ and $m \equiv n \pmod{\varphi(p^{e+1})}$ with Euler's totient function φ. For details on generalized Voronoï's congruences and p-adic L-functions, see, e.g., [27, 5] and [16, 19, 33], respectively.

Based on Proposition 4.4, we can state the following theorem:

Theorem 4.5. *Let p be an odd prime with $p \equiv 1 \pmod 4$ and s' be any fixed quadratic non-residue modulo p. Then $p \mid u$ is equivalent to each of*

$$\text{(i)}\quad \sum_{i=0}^{p-2}\frac{(-1)^i}{g_i}\left\lfloor\frac{s'g_i}{p}\right\rfloor \equiv 0 \pmod{p};$$

$$\text{(ii)}\quad \sum_{j=0}^{\mu-1}\frac{(-1)^j}{g_j}\left\lfloor\frac{s'g_j}{p}\right\rfloor \equiv \frac{(s'-1)g}{g+1} \pmod{p}.$$

Proof. Set $k=\mu$ and $a=s'$ in Proposition 4.4 (i). Noting that $g_i^{\mu} \equiv (-1)^i \pmod{p}$ and $s'^{\mu} \equiv \left(\frac{s'}{p}\right) \equiv -1 \pmod{p}$, we obtain

$$-2\frac{B_\mu}{\mu} \equiv \sum_{i=0}^{p-2}(s'g_i)^{\mu-1}\left\lfloor\frac{s'g_i}{p}\right\rfloor \equiv -\frac{1}{s'}\sum_{i=0}^{p-2}\frac{(-1)^i}{g_i}\left\lfloor\frac{s'g_i}{p}\right\rfloor \pmod{p},$$

and this congruence proves that $p \mid B_\mu$ is equivalent to (i). Similar to the above, setting $k = \mu$ and $a = s'$ in Proposition 4.4 (ii), we have, since $s'^{\mu} \equiv -1 \pmod{p}$,

$$\begin{aligned} -2\frac{B_\mu}{\mu} &\equiv 2\sum_{j=0}^{\mu-1}(s'g_j)^{\mu-1}\left\lfloor \frac{s'g_j}{p} \right\rfloor + \frac{2(s'-1)s'^{\mu-1}}{g^{\mu-1}-1} \\ &\equiv -\frac{2}{s'}\sum_{j=0}^{\mu-1}\frac{(-1)^j}{g_j}\left\lfloor \frac{s'g_j}{p} \right\rfloor + \frac{2(s'-1)g}{s'(g+1)} \pmod{p}. \end{aligned}$$

Multiplying this by $s'/2$, we can confirm that $p \mid B_\mu$ is equivalent to (ii). □

§ 4.3 Next we introduce Vandiver's curious congruence which, generally speaking, involves two Bernoulli numbers having symmetric indices with respect to the midpoint μ of the interval $[0, p-1]$.

For arbitrary positive integers m and a, we define the function $\lambda(m, a)$ by

$$\lambda(m,a) := \begin{cases} 0 \quad \text{for } m = 1; \\ \sum' \dfrac{\xi^a - 1}{\xi^p - 1} \quad \text{for } m \geq 2, \end{cases}$$

where p is a fixed odd prime and the sum $\sum'$ is taken over all the mth roots ξ $(\neq 1)$ of unity. Using this function, Vandiver [31, 32] proved the following proposition:

Proposition 4.6. *Let p be an odd prime and let a and k be arbitrary integers with $1 \leq a \leq p-1$ and $1 \leq k < p-1$. Then*

$$a\frac{B_k}{k} + a^{k+1}\frac{B_{p-1-k}}{p-1-k} \equiv \sum_{m=1}^{p-1} m^k \lambda(m,a) \pmod{p}. \tag{4.6}$$

We now assume that $p \geq 5$ and $k \geq 2$ is even. Given arbitrary positive integers m and a prime to p, let $X := X_m(a)$ and $Y := Y_m(a)$ be solutions of the linear Diophantine equation

$$pX - mY = a, \quad 1 \leq X \leq m, \quad 1 \leq Y \leq p-1.$$

As is easily seen, these solutions are uniquely determined depending on m and a. In particular, if $a = 1$, then we have

$$X_m(1) = m - \frac{m\overline{m} - 1}{p} \quad \text{and} \quad Y_m(1) = p - \overline{m},$$

where $\overline{m}$ is the modular inverse of m modulo p, i.e., the integer satisfying $m\overline{m} \equiv 1 \pmod{p}$ and $1 \leq \overline{m} \leq p-1$.

Since $\{pk+m\mathbb{Z} \mid k=1,2,...,m-1\} = \{k+m\mathbb{Z} \mid k=1,2,..,m-1\}$, it is possible to rewrite $\lambda(m,a)$ as

$$\lambda(m,a) = \sum{}' \frac{\xi^{pX_m(a)}-1}{\xi^p-1} = \sum{}' \frac{\xi^{X_m(a)}-1}{\xi-1} = m - X_m(a).$$

If k is even, then $p-1 \nmid k+1$, and so we have $S_{k+1}(p) \equiv 0 \pmod p$ by (4.2) in Proposition 4.1. Therefore, (4.6) leads to

$$\begin{aligned} a\frac{B_k}{k} + a^{k+1}\frac{B_{p-1-k}}{p-1-k} &\equiv \sum_{m=1}^{p-1} m^k(m - X_m(a)) \\ &\equiv S_{k+1}(p) - \sum_{m=1}^{p-1} m^k X_m(a) \equiv -\sum_{m=1}^{p-1} m^k X_m(a) \qquad (4.7) \\ &\equiv -\sum_{m=1}^{p-1} m^k \frac{mY_m(a)+a}{p} \pmod p. \end{aligned}$$

Making use of this congruence, we can prove the following theorem:

Theorem 4.7. *Let p be an odd prime with $p \equiv 1 \pmod 4$ and r' be any fixed quadratic residue modulo p. Then $p \mid u$ is equivalent to each of*

$$\text{(i)} \quad \sum_r X_r(r') \equiv \sum_s X_s(r') \pmod p;$$

$$\text{(ii)} \quad \sum_r rY_r(r') \equiv \sum_s sY_s(r') \pmod{p^2}.$$

Proof. Set $a = r'$ and $k = \mu$ in (4.7). Since $\left(\frac{r'}{p}\right) \equiv r'^{\mu} \equiv 1 \pmod p$ and $m^{\mu} \equiv \left(\frac{m}{p}\right) \pmod p$, we have

$$2r'\frac{B_\mu}{\mu} \equiv -\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)X_m(r') \equiv -\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)\frac{mY_m(r')+r'}{p} \pmod p, \qquad (4.8)$$

which proves that $p \mid B_\mu$ is equivalent to each of (i) and (ii). Here we used the fact that $\sum_{m=1}^{p-1}\left(\frac{m}{p}\right) = 0$, after multiplying (4.8) by p, in order to derive (ii). □

Theorem 4.8. *If $p \equiv 1 \pmod 4$, then $p \mid u$ is equivalent to each of*

$$\text{(i)} \quad \sum_r \frac{r\overline{r}-1}{p} \equiv \sum_s \frac{s\overline{s}-1}{p} \pmod p;$$

$$\text{(ii)} \quad \sum_r r\overline{r} \equiv \sum_s s\overline{s} \pmod{p^2}.$$

Proof. In particular, if we take $r' = 1$ in (4.8), then, using $Y_m(1) = p - \overline{m}$ and the fact that $\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) m = 0$, we have

$$\begin{aligned} 2\frac{B_\mu}{\mu} &\equiv -\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \frac{m(p-\overline{m})+1}{p} \equiv -\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \left(m - \frac{m\overline{m}-1}{p}\right) \\ &\equiv \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \frac{m\overline{m}-1}{p} \equiv \sum_{r} \frac{r\overline{r}-1}{p} - \sum_{s} \frac{s\overline{s}-1}{p} \pmod{p}, \end{aligned} \tag{4.9}$$

which shows that $p \mid B_\mu$ is equivalent to (i). Also, multiplying (i) by p and using $\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) = 0$ again, we can confirm that (i) is equivalent to (ii). □

By shortening intervals for r and s in Theorem 4.8 we have the following:

Theorem 4.9. *If* $p \equiv 1 \pmod 4$*, then* $p \mid u$ *is equivalent to each of*

(i) $$\sum_{0<r<p/2} \left(\frac{2(r\overline{r}-1)}{p} - (r+\overline{r})\right) \equiv \sum_{0<s<p/2} \left(\frac{2(s\overline{s}-1)}{p} - (s+\overline{s})\right) \pmod{p};$$

(ii) $$\sum_{0<r<p/2} (2r\overline{r} - (r+\overline{r})p) \equiv \sum_{0<s<p/2} (2s\overline{s} - (s+\overline{s})p) \pmod{p^2}.$$

Proof. Noting that $\overline{p-m} = p - \overline{m}$ and $\left(\frac{p-m}{p}\right) = \left(\frac{m}{p}\right)$ for each $m = 1, 2, ..., \mu - 1$, we obtain from (4.9) that

$$\begin{aligned} 2\frac{B_\mu}{\mu} &\equiv \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \frac{m\overline{m}-1}{p} \\ &\equiv \sum_{m=1}^{\mu} \left(\frac{m}{p}\right) \left(\frac{m\overline{m}-1}{p} + \frac{(p-m)(p-\overline{m})-1}{p}\right) \\ &\equiv \sum_{m=1}^{\mu} \left(\frac{m}{p}\right) \left(\frac{2(m\overline{m}-1)}{p} - (m+\overline{m})\right) \pmod{p}, \end{aligned}$$

which proves that $p \mid B_\mu$ is equivalent to (i). Also, multiplying (i) by p and using $\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) = 0$, it can be easily confirmed that (i) is equivalent to (ii). □

§ 4.4 In this subsection we will observe congruence (4.9) once more from a slightly different viewpoint using a primitive root g modulo p and derive several conditions equivalent to $p \mid B_\mu$.

Since $\overline{g_i} = g_{p-1-i}$ and $g_i = g^i - \lfloor g^i/p \rfloor p$ for each $i = 0, 1, ..., p-2$, we get

$$\begin{aligned} g_i\overline{g_i} = g_i g_{p-1-i} &= \left(g^i - \left\lfloor \frac{g^i}{p} \right\rfloor p\right)\left(g^{p-1-i} - \left\lfloor \frac{g^{p-1-i}}{p} \right\rfloor p\right) \\ &\equiv g^{p-1} - \left(g^i \left\lfloor \frac{g^{p-1-i}}{p} \right\rfloor + g^{p-1-i} \left\lfloor \frac{g^i}{p} \right\rfloor\right) p \pmod{p^2}. \end{aligned}$$

Subtracting 1 from both ends and dividing by p, this congruence gives

$$\frac{g_i\overline{g_i} - 1}{p} \equiv q_p(g) - \left(g_i \left\lfloor \frac{g^{p-1-i}}{p} \right\rfloor + \overline{g_i} \left\lfloor \frac{g^i}{p} \right\rfloor\right) \pmod{p}. \tag{4.10}$$

By making use of (4.10), we will prove the following theorem:

Theorem 4.10. *If* $p \equiv 1 \pmod 4$*, then* $p \mid u$ *is equivalent to each of*

$$\text{(i)} \quad \sum_{i=0}^{p-2} (-1)^i \left(g_i \left\lfloor \frac{g^{p-1-i}}{p} \right\rfloor + \overline{g_i} \left\lfloor \frac{g^i}{p} \right\rfloor\right) \equiv 0 \pmod{p};$$

$$\text{(ii)} \quad \sum_{i=0}^{p-2} (-1)^i g_i \overline{g_i} \equiv 0 \pmod{p^2}.$$

Proof. Since $g_i \neq g_j$ unless $p-1 \mid i-j$, we have $\{g_i \mid 0 \leq i \leq p-2\} = \{1, 2, ..., p-1\}$, and thus we obtain from (4.9) and (4.10) that

$$\begin{aligned} 2\frac{B_\mu}{\mu} &\equiv \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \frac{m\overline{m} - 1}{p} \equiv \sum_{i=0}^{p-2} \left(\frac{g_i}{p}\right) \frac{g_i\overline{g_i} - 1}{p} \\ &\equiv \sum_{i=0}^{p-2} (-1)^i \left(q_p(g) - g_i \left\lfloor \frac{g^{p-1-i}}{p} \right\rfloor - \overline{g_i} \left\lfloor \frac{g^i}{p} \right\rfloor\right) \\ &\equiv -\sum_{i=0}^{p-2} (-1)^i \left(g_i \left\lfloor \frac{g^{p-1-i}}{p} \right\rfloor + \overline{g_i} \left\lfloor \frac{g^i}{p} \right\rfloor\right) \equiv 0 \pmod{p}, \end{aligned}$$

which proves that $p \mid B_\mu$ is equivalent to (i). Also, congruence (ii) can be deduced from this if we multiply by p and use the fact that $\sum_{i=0}^{p-2} \left(\frac{g_i}{p}\right) = 0$. □

We note that Theorem 4.10 (ii) is actually the same as Theorem 4.8 (ii), because $\left(\frac{g_i}{p}\right) = (-1)^i$ holds for any integer i.

Theorem 4.11. *If* $p \equiv 1 \pmod 4$*, then* $p \mid u$ *is equivalent to each of*

$$\text{(i)} \quad \sum_{j=1}^{\mu-1} (-1)^j \left(g_j \left\lfloor \frac{g^{p-1-j}}{p} \right\rfloor + \overline{g_j} \left\lfloor \frac{g^j}{p} \right\rfloor\right) \equiv -\left(q_p(g) + 1\right) \pmod{p};$$

$$\text{(ii)} \quad \sum_{j=1}^{\mu-1} (-1)^j g_j \overline{g_j} \equiv p - 1 \pmod{p^2}.$$

Proof. For brevity, set $T_i := g_i\lfloor g^{p-1-i}/p\rfloor + \overline{g_i}\lfloor g^i/p\rfloor$. Since $g_0 = g^0 = 1$, $g_\mu = p-1$ and $(g^\mu+1)/p \equiv -q_p(g)/2 \pmod p$, we have $T_0 = \lfloor g^{p-1}/p\rfloor = q_p(g)$ and

$$\begin{aligned} T_\mu = 2g_\mu\left\lfloor\frac{g^\mu}{p}\right\rfloor &\equiv -2\left(\frac{g^\mu+1}{p}-1\right) \equiv -2\left(-\frac{1}{2}q_p(g)-1\right) \\ &\equiv q_p(g)+2 \pmod p, \end{aligned}$$

which yield $T_0+T_\mu \equiv 2(q_p(g)+1) \pmod p$. Also, since $(-1)^iT_i = (-1)^{p-1-i}T_{p-1-i}$ $(1 \le i \le p-2;\ i \ne \mu)$, we obtain from Theorem 4.10 (i) that

$$\sum_{i=0}^{p-2}(-1)^iT_i \equiv 2(q_p(g)+1) + 2\sum_{j=1}^{\mu-1}(-1)^jT_j \equiv 0 \pmod p,$$

which gives (i) after dividing by 2. On the other hand, using the congruence

$$g_0g_{p-1} + (-1)^\mu g_\mu^2 = 1+(p-1)^2 \equiv -2(p-1) \pmod{p^2},$$

we get from Theorem 4.10 (ii) that

$$\sum_{i=0}^{p-2}(-1)^ig_i\overline{g_i} \equiv -2(p-1) + 2\sum_{j=1}^{\mu-1}(-1)^jg_j\overline{g_j} \equiv 0 \pmod{p^2}.$$

Dividing this by 2, we can immediately derive (ii), as desired. □

§ 4.5 In this subsection we will utilize some classical congruences discovered by E. Lehmer and derive several conditions equivalent to $p \mid B_\mu$, and hence to $p \mid u$.

At first, we define the functions such that

$$\begin{aligned} Z_2(x) :=& 2^x - 1; \\ Z_3(x) :=& \frac{1}{2}\left(3^x-1\right); \\ Z_4(x) :=& \frac{1}{2}\left(2^x-1\right)\left(2^{x-1}+1\right); \\ Z_6(x) :=& \frac{1}{2}\left(6^{x-1}+3^{x-1}+2^{x-1}-1\right). \end{aligned}$$

Using these functions, E. Lehmer established in [22] the following proposition:

Proposition 4.12. *Let p be an odd prime and $k \ge 2$ be an even integer such that $p-1 \nmid k-2$. Then it follows that for each $\nu = 2,3,4,6$,*

$$Z_\nu(k)\frac{B_k}{k} \equiv \sum_{0<i<p/\nu}(p-i\nu)^{k-1} \pmod{p^2}, \tag{4.11}$$

provided that $p \ge 7$ for $\nu = 6$.

Lehmer's congruences (4.11) have played an important role for irregularity testing of primes as well as Voronoï's congruences introduced in Subsection 4.2. A generalized version of (4.11) for the square-modulus n^2 of any positive integer n can be found, e.g., in [3, 5].

The following lemma can be easily verified by using only basic properties of the Legendre symbol (for reference, see, e.g., [29, 25]).

Lemma 4.13. *Let p be an odd prime with $p \equiv 1 \pmod 4$. Then we have*

$$\text{(i)} \quad \left(\frac{2}{p}\right) = -1 \ \textit{if} \ p \equiv 5 \pmod 8; \qquad \text{(ii)} \quad \left(\frac{3}{p}\right) = -1 \ \textit{if} \ p \equiv 5 \pmod{12};$$

$$\text{(iii)} \quad \left(\frac{6}{p}\right) = 1 \ \textit{if} \ p \equiv 1, 5 \pmod{24}.$$

This lemma will be used in the next theorem in order to evaluate values of $Z_\nu(k)$ at $k = \mu$ modulo p.

Theorem 4.14. *Let p be an odd prime and let $\nu_1 := 2$ if $p \equiv 5 \pmod 8$, $\nu_2 := 3$ if $p \equiv 5 \pmod{12}$, $\nu_3 := 4$ if $p \equiv 5 \pmod 8$ and $\nu_4 := 6$ if $p \neq 5$ and $p \equiv 5 \pmod{24}$. Then $p \mid u$ is equivalent to*

$$\sum_{0<r<p/\nu_l} \frac{1}{r} \equiv \sum_{0<s<p/\nu_l} \frac{1}{s} \pmod p, \quad l = 1, 2, 3, 4. \tag{4.12}$$

Proof. Take $k = \mu$ in (4.11). Then we have for each $l = 1, 2, 3, 4$,

$$Z_{\nu_l}(\mu) \frac{B_\mu}{\mu} \equiv \sum_{0<i<p/\nu_l} (p - i\nu_l)^{\mu-1} \equiv -\nu_l^{\mu-1} \sum_{0<i<p/\nu_l} i^{\mu-1} \pmod p. \tag{4.13}$$

Here we see from Lemma 4.13 that

$$\begin{aligned} Z_{\nu_1}(\mu) &= 2^\mu - 1 \equiv -2 \pmod p; \\ Z_{\nu_2}(\mu) &= \frac{1}{2}\left(3^\mu - 1\right) \equiv -1 \pmod p; \\ Z_{\nu_3}(\mu) &= \frac{1}{2}\left(2^\mu - 1\right)\left(2^{\mu-1} + 1\right) \equiv -\frac{1}{2} \pmod p; \\ Z_{\nu_4}(\mu) &= \frac{1}{2}\left(6^{\mu-1} + 3^{\mu-1} + 2^{\mu-1} - 1\right) \equiv -\frac{5}{6} \pmod p. \end{aligned}$$

These congruences show that $p \nmid Z_{\nu_l}(\mu)$ for all $l = 1, 2, 3, 4$, and thus we can state from congruence (4.13) that $p \mid B_\mu$ is equivalent to

$$\sum_{0<i<p/\nu_l} i^{\mu-1} \equiv \sum_{0<i<p/\nu_l} \left(\frac{i}{p}\right) \frac{1}{i} \equiv 0 \pmod p,$$

which proves (4.12), as desired. □

§ 4.6 Let G_n be the nth Genocchi number defined by the Taylor expansion

$$\frac{2x}{e^x+1}=\sum_{n=0}^{\infty}G_n\frac{x^n}{n!}\quad(|x|<\pi).$$

These numbers are integers and the first few of them are $0,1,-1,0,1,0,-3,0,17$ and so on. From the functional identity

$$2\left(\frac{x}{e^x-1}-\frac{2x}{e^{2x}-1}\right)=\frac{2x}{e^x+1},$$

we see that $G_n=2(1-2^n)B_n$ for any $n\geq 0$ and hence $G_n=0$ if $n\geq 3$ is odd.

Making use of the well-known recurrence relation

$$G_k+\frac{1}{2}\sum_{j=0}^{k-1}\binom{k}{j}G_jn^{k-j}=k\sum_{i=1}^{n-1}(-1)^ii^{k-1}\quad(n\geq 1,\text{ an odd})$$

and the von Staudt-Clausen theorem, it is easy to prove the following:

Proposition 4.15. *For an odd prime p and an integer $k\geq 2$, it follows that*

$$G_k\equiv k\sum_{i=1}^{p-1}(-1)^ii^{k-1}\pmod{p}.\tag{4.14}$$

Based on this proposition, we can derive the following theorem:

Theorem 4.16. *If $p\equiv 5\pmod 8$, then $p\mid u$ is equivalent to each of*

$$\text{(i)}\quad\sum_{\substack{0<r<p/2\\ r\text{ odd}}}\frac{1}{r}\equiv\sum_{\substack{0<s<p/2\\ s\text{ odd}}}\frac{1}{s}\pmod{p};$$

$$\text{(ii)}\quad\sum_{\substack{0<r<p/2\\ r\text{ even}}}\frac{1}{r}\equiv\sum_{\substack{0<s<p/2\\ s\text{ even}}}\frac{1}{s}\pmod{p}.$$

Proof. Set $k=\mu$ in (4.14). If $p\equiv 5\pmod 8$, then $2^\mu\equiv\left(\frac{2}{p}\right)\equiv -1\pmod p$. Also, since $\mu\equiv -1/2\pmod p$, $i^{\mu-1}\equiv\left(\frac{i}{p}\right)\frac{1}{i}\pmod p$ and $(-1)^{p-i}\left(\frac{p-i}{p}\right)=-(-1)^i\left(\frac{i}{p}\right)$ for $i=1,2,...,p-1$, we have

$$\begin{aligned}G_\mu\equiv 4B_\mu\equiv -\frac{1}{2}\sum_{i=1}^{p-1}\frac{(-1)^i}{i}\left(\frac{i}{p}\right)&\equiv-\sum_{0<i<p/2}\frac{(-1)^i}{i}\left(\frac{i}{p}\right)\\ \equiv-\sum_{0<r<p/2}\frac{(-1)^r}{r}+\sum_{0<s<p/2}\frac{(-1)^s}{s}&\pmod{p}.\end{aligned}\tag{4.15}$$

On the other hand, considering (4.13) with $l = 1$ (and hence $\nu_1 = 2$) and multiplying by 2, it follows that

$$\begin{aligned} 2Z_2(\mu)\frac{B_\mu}{\mu} &\equiv 8B_\mu \equiv -2^\mu \sum_{0<i<p/2} i^{\mu-1} \equiv \sum_{0<i<p/2} \left(\frac{i}{p}\right)\frac{1}{i} \\ &\equiv \sum_{0<r<p/2} \frac{1}{r} - \sum_{0<s<p/2} \frac{1}{s} \pmod{p}. \end{aligned} \tag{4.16}$$

Adding (4.15) to (4.16) and dividing by 2, we get

$$6B_\mu \equiv \sum_{\substack{0<r<p/2 \\ r \text{ odd}}} \frac{1}{r} - \sum_{\substack{0<s<p/2 \\ s \text{ odd}}} \frac{1}{s} \pmod{p},$$

which implies that $p \mid B_\mu$ is equivalent to (i). Also, subtracting (4.15) from (4.16) and dividing by 2, we get

$$2B_\mu \equiv \sum_{\substack{0<r<p/2 \\ r \text{ even}}} \frac{1}{r} - \sum_{\substack{0<s<p/2 \\ s \text{ even}}} \frac{1}{s} \pmod{p},$$

which proves that $p \mid B_\mu$ is equivalent to (ii). □

Theorem 4.17. *If $p \equiv 5 \pmod{8}$, then $p \mid u$ is equivalent to*

$$\sum_{0<r<p/2} q_p(r) \equiv \sum_{0<s<p/2} q_p(s) \pmod{p}. \tag{4.17}$$

Proof. As we have seen in (4.16), if $p \equiv 5 \pmod{8}$, then $p \mid B_\mu$ is equivalent to

$$\sum_{0<r<p/2} \frac{1}{r} \equiv \sum_{0<s<p/2} \frac{1}{s} \pmod{p},$$

and so we may state from Theorem 3.3 (ii) that $p \mid B_\mu$ is equivalent to (4.17). □

§ 4.7 For further discussion, we define the following two special polynomials in the ring $\mathbb{Z}[x]$ over the integers:

$$\begin{aligned} P(x) :=& g_0 + g_1 x + \cdots + g_{p-2}x^{p-2}; \\ Q(x) :=& s_0 + s_1 x + \cdots + s_{p-2}x^{p-2}, \end{aligned}$$

where $s_i := (gg_i - g_{i+1})/p$ for each $i = 0, 1, ..., p-2$.

Incidentally, we wish to mention that these polynomials have been utilized in order to formulate the relative class number h_p^- of the cyclotomic field $\mathbb{Q}(\zeta)$ defined by ζ, a primitive pth root of unity. Indeed, Kummer (in 1851) and Inkeri (in 1955) established the following expressions (i) and (ii) of h_p^- used special values of $P(x)$ and $Q(x)$, respectively: let θ be a primitive $(p-1)$st root of unity. Then

$$\text{(i)}\quad h_p^- = \frac{(-1)^\mu}{(2p)^{\mu-1}} \prod_{k=0}^{\mu-1} P(\theta^{2k+1}); \quad \text{(ii)}\quad h_p^- = \frac{(-1)^\mu p}{2p^{\mu-1}(g^\mu+1)} \prod_{k=0}^{\mu-1} Q(\theta^{2k+1}).$$

For more details and related class number topics, see, e.g., [15, 23, 26, 33, 25, 8].

A basic relation between $P(x)$ and $Q(x)$ can be stated by

$$\frac{1}{p}(gx-1)P(x) = xQ(x) + \frac{1}{p}(x^{p-1}-1), \tag{4.18}$$

which is easily confirmed by direct calculation.

We now extract from [6, Section 3] two congruences expressing B_k/k by means of special values of $P(x)$ and $Q(x)$, and reprove them for the sake of completeness.

Proposition 4.18. *Let p be an odd prime and $k \geq 2$ be an even integer with $p-1 \nmid k$. Then we have*

$$\text{(i)}\quad \frac{1}{p}P(g^{k-1}) \equiv \frac{B_k}{k} + \frac{k-1}{g^k-1} q_p(g) \pmod{p};$$
$$\text{(ii)}\quad Q(g^{k-1}) \equiv \frac{g^k-1}{g^{k-1}} \cdot \frac{B_k}{k} \pmod{p}.$$

Proof. At first, we mention the following congruence proved in [4, Theorem 1.1]:

$$\frac{B_k}{k} \equiv \frac{g^k}{g^k-1} q_p(g) - \sum_{i=1}^{p-1} g^{(k-1)i} \left\lfloor \frac{g^i}{p} \right\rfloor \pmod{p}. \tag{4.19}$$

Since $\lfloor g^i/p \rfloor = (g^i - g_i)/p$, $g_{p-1} = g_0 = 1$ and $q_p(g^{k-1}) \equiv (k-1)q_p(g) \pmod{p}$ by Lemma 3.2, we obtain from (4.19) that

$$\begin{aligned}\frac{B_k}{k} \equiv & \frac{g^k}{g^k-1} q_p(g) - \frac{1}{p}\left(\sum_{i=1}^{p-1} g^{ki} - \sum_{i=1}^{p-1} g^{(k-1)i} g_i\right) \\ \equiv & \frac{g^k}{g^k-1} q_p(g) - \frac{g^k}{g^k-1} q_p(g^k) + \frac{1}{p}P(g^{k-1}) + q_p(g^{k-1}) \\ \equiv & -\frac{k-1}{g^k-1} q_p(g) + \frac{1}{p}P(g^{k-1}) \pmod{p},\end{aligned}$$

which gives (i). For the proof of (ii), take $x = g^{k-1}$ in (4.18). That is,

$$\frac{1}{p}(g^k-1)P(g^{k-1}) = g^{k-1}Q(g^{k-1}) + q_p(g^{k-1}),$$

which leads to (ii) by using (i) and $q_p(g^{k-1}) \equiv (k-1)q_p(g) \pmod{p}$ again. □

We note that Proposition 4.18 (ii) is just a special case of Voronoï's congruences mentioned in Subsection 4.2. Indeed, if we take $a = g$ in Proposition 4.4 (i), then, noticing the fact such that $Q(g^{k-1}) \equiv \sum_{i=0}^{p-2} s_i g_i^{k-1} \pmod{p}$, we have

$$\begin{aligned}(g^k - 1)\frac{B_k}{k} &\equiv \sum_{i=0}^{p-2}(gg_i)^{k-1}\left\lfloor \frac{gg_i}{p} \right\rfloor \equiv g^{k-1}\sum_{i=0}^{p-2} g_i^{k-1}\frac{gg_i - g_{i+1}}{p} \\ &\equiv g^{k-1}Q(g^{k-1}) \pmod{p},\end{aligned}$$

which is exactly the same as Proposition 4.18 (ii). As is well-known, this congruence is very practical for the irregularity testing of primes by computer, in view of the running time of operations. More detailed explanations can be found in the excellent paper [13] by Buhler and Harvey.

Using Proposition 4.18, we may state the following theorem:

Theorem 4.19. *If $p \equiv 1 \pmod{4}$, then $p \mid u$ is equivalent to each of*

$$\text{(i)}\quad \frac{1}{p}P(g^{\mu-1}) \equiv \frac{3}{4}q_p(g) \pmod{p};$$

$$\text{(ii)}\quad Q(g^{\mu-1}) \equiv 0 \pmod{p}.$$

Proof. Taking $k = \mu$ in Proposition 4.18 and noting that $(\mu - 1)/(g^\mu - 1) \equiv 3/4 \pmod{p}$, we immediately see that $p \mid B_\mu$ is equivalent to each of (i) and (ii). □

The following is just a transformation of Proposition 4.18:

Proposition 4.20. *Let p be an odd prime and $k \geq 2$ be an even integer with $p - 1 \nmid k$. Then we have*

$$\text{(i)}\quad \frac{B_k}{k} \equiv \frac{2}{p}\sum_{j=0}^{\mu-1} g_j g^{(k-1)j} - \frac{k-1}{g^k - 1}q_p(g) + \frac{2}{g^{k-1} - 1} \pmod{p};$$

$$\text{(ii)}\quad \frac{B_k}{k} \equiv \frac{2g^{k-1}}{g^k - 1}\left(\sum_{j=0}^{\mu-1} s_j g^{(k-1)j} + \frac{g-1}{g^{k-1} - 1}\right) \pmod{p}.$$

Proof. Since $g_j + g_{j+\mu} \equiv g^j(1 + g^\mu) \equiv 0 \pmod{p}$ and $1 \leq g_j, g_{\mu+j} \leq p - 1$ for each $j = 0, 1, ..., \mu - 1$, we see that $g_j + g_{j+\mu} = p$, and hence

$$P(x) = \sum_{j=0}^{\mu-1} g_j x^j + \sum_{j=0}^{\mu-1}(p - g_j)x^{\mu+j} = (1 - x^\mu)\sum_{j=0}^{\mu-1} g_j x^j + px^\mu\frac{1 - x^\mu}{1 - x}.$$

Putting here $x = g^{k-1}$ for an even $k \geq 2$ and dividing by p, we get

$$\begin{aligned}\frac{1}{p}P(g^{k-1}) &= \frac{1}{p}(1 - g^{(k-1)\mu})\sum_{j=0}^{\mu-1} g_j g^{(k-1)j} + g^{(k-1)\mu}\frac{1 - g^{(k-1)\mu}}{1 - g^{k-1}} \\ &\equiv \frac{2}{p}\sum_{j=0}^{\mu-1} g_j g^{(k-1)j} + \frac{2}{g^{k-1} - 1} \pmod{p},\end{aligned}$$

and this proves (i) by Proposition 4.18 (i). On the other hand, since $g_{k+\mu} = p - g_k$ $(0 \leq k \leq \mu)$, it follows that

$$s_j + s_{j+\mu} = \frac{g_j g - g_{j+1}}{p} + \frac{(p - g_j)g - (p - g_{j+1})}{p} = g - 1, \qquad (4.20)$$

and therefore, $Q(x)$ can be written as

$$\begin{aligned} Q(x) &= \sum_{j=0}^{\mu-1} (s_j x^j + s_{j+\mu} x^{j+\mu}) = \sum_{j=0}^{\mu-1} (s_j + (g - 1 - s_j)x^\mu)\, x^j \\ &= (1 - x^\mu) \sum_{j=0}^{\mu-1} s_j x^j + (g-1)x^\mu \frac{1 - x^\mu}{1 - x}. \end{aligned}$$

Here, we set $x = g^{k-1}$ for an even $k \geq 2$. Since $g^{(k-1)\mu} \equiv (-1)^{k-1} \equiv -1 \pmod{p}$, it is shown that

$$\begin{aligned} Q(g^{k-1}) &= \left(1 - g^{(k-1)\mu}\right) \sum_{j=0}^{\mu-1} s_j g^{(k-1)j} + (g-1) g^{(k-1)\mu} \frac{1 - g^{(k-1)\mu}}{1 - g^{k-1}} \\ &\equiv 2 \sum_{j=0}^{\mu-1} s_j g^{(k-1)j} + \frac{2(g-1)}{g^{k-1} - 1} \pmod{p}, \end{aligned}$$

which gives (ii) from Proposition 4.18 (ii). □

Theorem 4.21. *If $p \equiv 1 \pmod 4$, then $p \mid u$ is equivalent to each of*

$$\text{(i)} \quad \frac{1}{p} \sum_{j=0}^{\mu-1} g_j g^{(\mu-1)j} \equiv \frac{3}{8} q_p(g) + \frac{g}{g+1} \pmod{p};$$

$$\text{(ii)} \quad \sum_{j=0}^{\mu-1} s_j \left(-\frac{1}{g}\right)^j \equiv \frac{g(g-1)}{g+1} \pmod{p}.$$

Proof. Take $k = \mu$ in congruences (i) and (ii) in Proposition 4.20. Since $g^\mu \equiv -1 \pmod{p}$, $\mu \equiv -1/2 \pmod{p}$ and $2g^{\mu-1}/(g^\mu - 1) \equiv 1/g \not\equiv 0 \pmod{p}$, it can be easily confirmed that $p \mid B_\mu$ is equivalent to each of (i) and (ii). □

We now consider a special case where p has $g = 2$ as a primitive root. In this case, the value of s_j can be evaluated as follows:

Lemma 4.22. *For an odd prime p, if 2 is a primitive root modulo p, then it follows that for each $j = 0, 1, ..., \mu - 1$,*

$$s_j = 1 - s_{j+\mu} = \begin{cases} 0 & \textit{if } \lfloor 2^{j+1}/p \rfloor \textit{ is even;} \\ 1 & \textit{if } \lfloor 2^{j+1}/p \rfloor \textit{ is odd.} \end{cases}$$

Proof. In general, since $g_j = g^j - \lfloor g^j/p \rfloor p$, we have

$$s_j = \frac{1}{p}\left(\left(g^j - \left\lfloor \frac{g^j}{p} \right\rfloor p\right) g - \left(g^{j+1} - \left\lfloor \frac{g^{j+1}}{p} \right\rfloor p\right)\right) = \left\lfloor \frac{g^{j+1}}{p} \right\rfloor - g\left\lfloor \frac{g^j}{p} \right\rfloor.$$

In particular, if $g = 2$, then we see that $s_j \in \{0, 1\}$ from (4.20) and the last term on the right-hand side of this identity is always even, so the lemma follows. □

Note that $\lfloor 2^{j+1}/p \rfloor$ is odd if and only if the least positive residue of 2^{i+1} modulo p is odd, because we have $2^{j+1} - \lfloor 2^{j+1}/p \rfloor p \equiv \lfloor 2^{j+1}/p \rfloor \pmod 2$.

Theorem 4.23. *Let p be an odd prime with $p \equiv 1 \pmod 4$. If 2 is a primitive root modulo p, then $p \mid u$ is equivalent to each of*

$$\text{(i)} \quad \sum_{j=0}^{\mu-1} s_j \mu^j \equiv \frac{2}{3} \pmod{p};$$

$$\text{(ii)} \quad \sum_{j=0}^{\mu-1} s_{j+\mu} \mu^j \equiv \frac{2}{3} \pmod{p}.$$

Proof. Take $g = 2$ in Theorem 4.21 (ii). Since $(-1/2)^j \equiv \mu^j \pmod p$, we may immediately conclude that $p \mid B_\mu$ is equivalent to (i). For the proof of (ii), substitute $s_j = 1 - s_{j+\mu}$ into (i). The condition $g = 2$ gives $\left(\frac{2}{p}\right) = 2^\mu = -1$ and hence $\mu^\mu \equiv (-1/2)^\mu \equiv -1 \pmod p$, so we have $\sum_{j=0}^{\mu-1} \mu^j = (1 - \mu^\mu)/(1 - \mu) \equiv 4/3 \pmod p$. By using this fact we can deduce

$$\sum_{j=0}^{\mu-1} s_{j+\mu} \mu^j \equiv \frac{1 - \mu^\mu}{1 - \mu} - \frac{2}{3} \equiv \frac{4}{3} - \frac{2}{3} \equiv \frac{2}{3} \pmod{p},$$

which proves that (i) is equivalent to (ii), as desired. □

Since $s_j + s_{j+\mu} = 1$ from (4.20), we notice that more than $\mu/2$ terms in the sum on the left-hand side of either (i) or (ii) in Theorem 4.23 vanish and this fact may be useful for practical testing by computer as to whether $p \mid u$ is false or not.

We note that if $p \equiv 1 \pmod 8$, then $\left(\frac{2}{p}\right) = 1$, so that the integer 2 is not a primitive root modulo p. Therefore, as a criterion for the AAC conjecture, we can apply Theorem 4.23 only for primes $p \equiv 5 \pmod 8$ having a primitive root $g = 2$ such as $p = 5, 13, 29, 37, 53, 61, 101$ and so on. Unfortunately, it is not known whether there exist infinitely many such primes, and this problem is still open as a part of the famous Artin conjecture on primitive roots.

Acknowledgements. The author would like to thank Karl Dilcher for a careful reading of the manuscript and many useful comments. Further thanks are due to Bruce Landman for his helpful suggestions for improving this article.

References

[1] T. Agoh, *A note on unit and class number of real quadratic fields*, Acta Math. Sinica (NS), **5** (1989), 281–288.

[2] T. Agoh, *On Fermat and Wilson quotients*, Expo. Math. **14** (1996), 145–170.

[3] T. Agoh, *Generalization of Lehmer's congruences for Bernoulli numbers*, C. R. Math. Rep. Acad. Sci. Canada, **22** (2000), 61–65.

[4] T. Agoh, *Congruences involving Bernoulli numbers and Fermat-Euler quotients*, J. Number Theory, **94** (2002), 1–9.

[5] T. Agoh, *Voronoï type congruence and its applications*, Eur. J. Pure Appl. Math. **1** (2008), 3–21.

[6] T. Agoh, *On the relative class number of special cyclotomic fields*, Math. for Appl. **1** (2012), 1–12.

[7] T. Agoh and T. Shoji, *Quadratic equations over finite fields and class numbers of real quadratic fields*, Monatsh. Math. **125** (1998), 279–292.

[8] T. Agoh and T. Taniguchi, *A study of Inkeri's class number formula*, Expo. Math. **24** (2006), 53–79.

[9] N. C. Ankeny, E. Artin, and S. Chowla, *The class number of real quadratic fields*, Proc. Nat. Acad. Sci. USA, **37** (1951), 524–525.

[10] N. C. Ankeny, E. Artin, and S. Chowla, *The class number of real quadratic fields*, Ann. of Math. **56** (1952), 479–493.

[11] N. C. Ankeny and S. Chowla, *A further note on the class number of real quadratic fields*, Acta Arith. **7** (1962), 271–272.

[12] N. G. W. H. Beeger, *Quelques remarques sur les congruences* $r^{p-1} \equiv 1 \pmod{p^2}$ *et* $(p-1)! \equiv -1 \pmod{p^2}$, Mess. Math. **43** (1913), 72–85.

[13] J. P. Buhler and D. Harvey, *Irregular primes to* 163 *million*, Math. Comp. **80** (2011), 2435–2444.

[14] L. Carlitz, *Note on the class number of real quadratic fields*, Proc. Amer. Math. Soc. **4** (1953), 535–537.

[15] K. Inkeri, *Über die Klassenzahl des Kreiskörpers der* l^{ten} *Einheitswurzeln*, Ann. Acad. Sci. Fenn. Ser. A.I. **199** (1955), 1–12.

[16] K. Iwasawa, *Lectures on p-adic L-Functions*, Annals of Math. Studies, No.74, Princeton Univ. Press, Princeton, New Jersey, 1972.

[17] K. Iyanaga, *A recursive method to calculate the number of solutions of quadratic equations over finite fields*, Math. Comp. **64** (1995), 1319–1331.

[18] A. A. Kiselev, *An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers* (Russian), Doklady Akad. Nauk SSSR (N.S.), **61** (1948), 777–779.

[19] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Grad. Texts in Math. 58, Springer-Verlag, New York-Heidelberg-Berlin, 1984.

[20] M.-H. Le, *The number of solutions of a certain quadratic congruence related to the class number of* $\mathbf{Q}(\sqrt{p})$, Proc. Amer. Math. Soc. **117** (1993), 1–3.

[21] M.-H. Le, *Upper bounds for class numbers of real quadratic fields*, Acta Arith. **68** (1994), 141–144.

[22] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. **39** (1938), 350–359.

[23] D. H. Lehmer, *Prime factors of cyclotomic class numbers*, Math. Comp. **31** (1977), 599–607.

[24] M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1}-1)/p = q(a)$, Math. Annalen, **60** (1905), 471–490.

[25] P. Ribenboim, *Classical Theory of Algebraic Numbers*, UTX, Springer-Verlag, New York-Berlin-Heidelberg, 2001.

[26] L. Skula, *Another proof of Iwasawa's class number formula*, Acta Arith. **39** (1981), 1–6.

[27] I. Sh. Slavutskii, *Generalized Voronoï's congruence and the number of classes of ideals of an imaginary quadratic field, II* (Russian), Izv. Vyšš. Učebn. Zaved. Math. **4**(53) (1966), 118–126.

[28] I. Sh. Slavutskii, *Upper bounds and numerical calculation of the number of ideal classes of real quadratic fields*, Amer. Math. Soc. Transl. (2), **82** (1969), 67–71.

[29] J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill, New York-London, 1939.

[30] A. J. van der Poorten, H. J. J. Te Riele, and H. C. Williams, *Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 100 000 000 000*, Math. Comp. **70** (2001), 1311–1328; *Corrigenda and addition*, Math. Comp. **72** (2003), 521–523.

[31] H. S. Vandiver, *On congruences which relate the Fermat and Wilson quotients for the Bernoulli numbers*, Proc. Amer. Math. Soc. **35** (1949), 332–337.

[32] H. S. Vandiver, *On developments in an arithmetic theory of the Bernoulli and allied numbers*, Scripta Math. **25** (1961), 273–303; Reprint with some misprints corrected, 1–39.

[33] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer-Verlag, New York-Heidelberg-Berlin, 1996.