CONGRUENCES RELATED TO THE WILSON QUOTIENT

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

Received: 5/1/22, Accepted: 11/22/22, Published: 12/16/22

Abstract

The main purpose of this paper is to investigate various kinds of congruences related to the Wilson quotient by applying a Miki-type linear identity involving two different kinds of sums for Bernoulli numbers, and further by reflecting characteristics of quadratic residues and non-residues modulo p, where p is a prime number satisfying $p \equiv 1 \pmod 4$.

1. Introduction

Throughout this paper, we denote by B_n, $n = 0, 1, 2, \ldots$, the Bernoulli numbers defined by the generating function

$$\mathbb{B}(t) := \frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \quad \text{with} \quad |t| < 2\pi.$$

It is easy to confirm that $B_{2n+1} = 0$ and $(-1)^{n-1} B_{2n} > 0$ for all integers $n \geq 1$. The most basic recurrence relation for these numbers is

$$B_0 = 1, \quad \sum_{i=0}^{n} \binom{n}{i} B_i = B_n \quad (n \geq 2). \tag{1.1}$$

As is well-known, the von Staudt-Clausen theorem asserts that

$$B_{2n} + \sum_{p-1 \mid 2n} \frac{1}{p} \in \mathbb{Z} \quad (n \geq 1), \tag{1.2}$$

where the sum is taken over all the primes p with $p-1 \mid 2n$. Therefore, denoting by $\mathbb{Z}_p$ the ring of p-adic integers, we see that if $p - 1 \nmid 2n$, then $B_{2n} \in \mathbb{Z}_p$; meanwhile, if $p - 1 \mid 2n$, then $pB_{2n} \in \mathbb{Z}_p$, precisely, $pB_{2n} \equiv -1 \pmod p$. On the other hand, the power sum of the first k positive integers such that

$$S_n(k) := 1^n + 2^n + \cdots + k^n \quad (n \geq 0;\, k \geq 1) \tag{1.3}$$

can be represented by means of Bernoulli numbers. In fact, Faulhaber's formula states that

$$\begin{aligned} S_n(k) &= \frac{1}{n+1}\sum_{i=1}^{n+1}\binom{n+1}{i}(k+1)^i B_{n+1-i} \\ &= \sum_{i=1}^{n+1}\frac{1}{i}\binom{n}{i-1}(k+1)^i B_{n+1-i}, \end{aligned} \tag{1.4}$$

which is an easy consequence of the functional identity $t\sum_{i=0}^{k} e^{it} = \mathbb{B}(t)(e^{(k+1)t}-1)$. In addition, the so-called Kummer's congruence states that, for a prime p and positive even integers n, m with $p-1 \nmid n$, if $n \equiv m \pmod{p-1}$, then

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p}. \tag{1.5}$$

It should be noted that this periodicity property was first discovered by von Staudt before Kummer. A detailed overview of the historical development process about this congruence can be found in the paper [29] by Slavutskii.

In number theory, Wilson's theorem asserts that if p is a prime, then

$$(p-1)! \equiv -1 \pmod{p},$$

which characterizes the primes. Based on this theorem, the Wilson quotient W_p is defined by

$$W_p := \frac{(p-1)!+1}{p} \in \mathbb{Z}.$$

A prime p that satisfies $W_p \equiv 0 \pmod{p}$ is called a *Wilson prime*. The known Wilson primes are only $5, 13$, and 563 (cf. A007540 in the OEIS [26]). Crandall, Dilcher, and Pomerance [14] have confirmed that there are no new Wilson primes up to 5×10^8. If there exists the fourth Wilson prime, then it must be greater than 2×10^{13} (cf. Costa et al. [13], 2012). The number of Wilson primes in an interval $[x, y]$ is expected to be about $\log(\log(y)/\log(x))$ (see the article "Wilson prime" in [11]). It is still open whether there exist infinitely many these primes — however, almost nothing is known about this problem.

On the other hand, Fermat's little theorem states that if p is a prime and $a \geq 1$ is an integer with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. According to this theorem, the Fermat quotient $q_p(a)$ with base a is defined by

$$q_p(a) := \frac{a^{p-1}-1}{p} \in \mathbb{Z}.$$

For $a, b \in \mathbb{Z}$ with $p \nmid ab$, we have $pq_p(a)q_p(b) = q_p(ab) - q_p(a) - q_p(b)$, which verifies that these quotients possess the logarithmic property. That is to say,

$$\begin{aligned} &\text{(i)} \quad q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}; \\ &\text{(ii)} \quad q_p(a^m) \equiv m q_p(a) \pmod{p} \quad (m \in \mathbb{Z},\ m > 0). \end{aligned} \tag{1.6}$$

Fermat quotients have been extensively studied in connection with the first case of Fermat's Last Theorem (for reference, see Ribenboim [27]). Especially, a prime p that satisfies $q_p(2) \equiv 0 \pmod{p}$ (resp. $q_p(3) \equiv 0 \pmod{p}$) is called a *Wieferich prime* (resp. a *Mirimanoff prime*). At the moment, the known Wieferich (resp. Mirimanoff) primes are only 1093 and 3511 (resp. 11 and 1006003) (cf. A001220 and A014127 in the OEIS [26]).

The Wilson quotient is deeply intertwined with Fermat quotients and Bernoulli numbers (for instance, see [1]). There are many interesting and remarkable results on the Wilson quotient, which were mainly explored by Lerch, Beeger, Glaisher, E. Lehmer, and other mathematicians. Inspired by these major results, in this paper we would like to investigate various kinds of congruences related to W_p based on our original perspective.

In Section 2, we recall some remarkable results and give an overview of them, offering full proofs for completeness. In Section 3, by applying a Miki-type linear identity for Bernoulli numbers involving two different kinds of sums (precisely, an ordinary sum and a binomial sum), we find special forms of congruences. In Section 4, by reflecting characteristics of quadratic residues and non-residues modulo p, $p \equiv 1 \pmod{4}$, we search for possible criteria for Wilson primes. In addition, we discuss certain expressions of W_p and the specified Bernoulli number $B_{(p-1)/2}$ by means of a primitive root g modulo p.

2. An Overview of Remarkable Results

In this section, we pick out some well-known remarkable results related to the Wilson quotient at our own discretion and give an overview of them, offering full proofs for the sake of completeness.

Among many known formulas for the Wilson quotient, the most celebrated one is Lerch's formula, which was published in 1905. This formula has been converted into various kinds of forms and used to search for diverse expressions of W_p.

Proposition 2.1 (Lerch [25])**.** *For an odd prime p, we have*

$$W_p \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p}. \tag{2.1}$$

Proof. The definitions of the Wilson and Fermat quotients yield that

$$\begin{aligned} q_p((p-1)!) = q_p(pW_p - 1) &= \frac{(pW_p - 1)^{p-1} - 1}{p} \\ &= \sum_{i=1}^{p-1} \binom{p-1}{i} (-1)^{p-1-i} p^{i-1} W_p^i. \end{aligned}$$

Since the logarithmic property (1.6) (i) provides the congruence

$$q_p((p-1)!) \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p},$$

we see that the above identity reduces to (2.1) modulo p. □

Proposition 2.2. *Lerch's formula* (2.1) *is equivalent to*

$$W_p \equiv B_{p-1} + \frac{1}{p} - 1 \pmod{p} \quad \text{(Glaisher [17], Beeger [9])}. \tag{2.2}$$

Proof. Assume that (2.1) holds. It implies that, by multiplying both sides by p,

$$pW_p \equiv p\sum_{a=1}^{p-1} q_p(a) \equiv \sum_{a=1}^{p-1}(a^{p-1}-1) \equiv S_{p-1}(p-1) - (p-1) \pmod{p^2}, \tag{2.3}$$

where $S_n(k)$ is the power sum as defined in (1.3). Using (1.4) and the fact that $\frac{1}{i}p^iB_{p-i} \equiv 0 \pmod{p^2}$ for all $i = 2, 3, \ldots, p$ except for $i = 1$, we get

$$S_{p-1}(p-1) = \sum_{i=1}^{p} \frac{1}{i}\binom{p-1}{i-1} p^i B_{p-i}. \equiv pB_{p-1} \pmod{p^2}. \tag{2.4}$$

Substituting (2.4) into (2.3) and dividing the whole by p lead to (2.2). The reverse implication is obvious in view of (2.3); so the proof is now complete. □

A generalization of (2.2) can be stated as follows.

Proposition 2.3. *For an integer $m > 0$, we have*

$$mW_p \equiv B_{m(p-1)} + \frac{1}{p} - 1 \pmod{p}. \tag{2.5}$$

Proof. Let us take $n = m(p-1)$ and $k = p-1$ in (1.4) to obtain

$$S_{m(p-1)}(p-1) = \sum_{i=1}^{m(p-1)+1} \frac{1}{i}\binom{m(p-1)}{i-1} p^i B_{m(p-1)+1-i}. \tag{2.6}$$

For simplicity, put $c_i := \frac{1}{i}p^iB_{m(p-1)+1-i}$ for $i \in I := \{1, 2, \ldots, m(p-1)+1\}$. We now suppose that $p^\alpha \parallel i$ for some integer $\alpha \geq 1$ and write i as $i = lp^\alpha$ with an integer $l \geq 1$, $p \nmid l$. Then one can find that $lp^\alpha - \alpha \geq p^\alpha - \alpha \geq 2$, because $p \geq 3$ and $pB_{m(p-1)+1-i} \in \mathbb{Z}_p$ by (1.2). So it follows that $c_i \equiv 0 \pmod{p^2}$ for all $i \in I\backslash\{1\}$. Based on this fact, identity (2.6) provides

$$S_{m(p-1)}(p-1) \equiv pB_{m(p-1)} \pmod{p^2}. \tag{2.7}$$

Next, taking $a = 1, 2, \ldots, p-1$ in (1.6) (ii) and summing up all of them, we have

$$\sum_{a=1}^{p-1} q_p(a^m) \equiv m \sum_{a=1}^{p-1} q_p(a) \pmod{p},$$

and thus, multiplying both sides by p,

$$\begin{aligned}\sum_{a=1}^{p-1} \left((a^m)^{p-1} - 1\right) &= S_{m(p-1)}(p-1) - (p-1) \\ &\equiv m\left(S_{p-1}(p-1) - (p-1)\right) \pmod{p^2}.\end{aligned}$$

Hence, by virtue of (2.2) and (2.3), we see that (2.7) leads to

$$pB_{m(p-1)} - (p-1) \equiv m\left(pB_{p-1} - (p-1)\right) \equiv mpW_p \pmod{p^2},$$

which is just the same as (2.5), after dividing the whole by p. □

By going through (2.2), we find that (2.5) is equivalent to

$$\frac{B_{m(p-1)} + \frac{1}{p} - 1}{m(p-1)} \equiv \frac{B_{p-1} + \frac{1}{p} - 1}{p-1} \pmod{p} \quad \text{(Johnson [19])},$$

which is valid for any integer $m > 0$. This Johnson's congruence is, in a sense, an extension of Kummer's (1.5) to the case where $p-1$ divides the indices. Note that Slavutskii [30] has investigated in detail such types of congruences for more higher power moduli of p, but it is rather intricate to restate here.

Proposition 2.4. *For integers $n, k > 0$, we have*

$$(n-k)W_p \equiv B_{n(p-1)} - B_{k(p-1)} \pmod{p}. \tag{2.8}$$

In particular,

$$W_p \equiv B_{2(p-1)} - B_{p-1} \pmod{p} \quad \text{(E. Lehmer [23])}.$$

Proof. Set $m = n$ and $m = k$ in (2.5). Taking the difference between these leads immediately to (2.8). The latter congruence is nothing but the special case of (2.8) for $n = 2$ and $k = 1$. □

In order to compute W_p, it requires an efficient calculation algorithm for $(p-1)!$. For that purpose, the formula given below is useful to reduce the computation of W_p to that of $\left(\frac{p-1}{2}\right)!$ (mod p^2). As has been reported, for instance, in [13], this formula appears without proof in Mathews' book [21], but it is unspecified about the name of the person who first discovered it. Later, Beeger [10] gave a complete proof and used it to compute W_p for all primes $p < 300$.

Proposition 2.5. *For brevity, let* $\nu := \frac{p-1}{2}$. *We have*

$$(p-1)! \equiv (-1)^{\nu}(\nu!)^2(2^p-1) \pmod{p^2}.$$

Proof. For a simple proof, we wish to apply a well-known formula such that

$$2q_p(2) \equiv -H_{\nu} \pmod{p} \quad \text{(Sylvester [31], Glaisher [18])}, \tag{2.9}$$

where H_n is the nth harmonic number, namely,

$$H_0 := 0. \quad H_n := \sum_{j=1}^{n} \frac{1}{j} \quad (n \geq 1).$$

Multiplying both sides of (2.9) by p, we have $2^p - 2 \equiv -pH_{\nu} \pmod{p^2}$. Therefore, it follows by direct calculation that

$$\begin{aligned}(p-1)! = \nu! \prod_{j=1}^{\nu}(p-j) &\equiv \nu!\left((-1)^{\nu}\nu! - (-1)^{\nu}\nu! pH_{\nu}\right) \\ &\equiv (-1)^{\nu}(\nu!)^2\left(1 - pH_{\nu}\right) \equiv (-1)^{\nu}(\nu!)^2(2^p-1) \pmod{p^2},\end{aligned}$$

as desired. □

It is worth mentioning that (2.9) is equivalent to

$$2q_p(2) \equiv H'_{p-1} \pmod{p} \quad \text{(Eisenstein [15])},$$

where H'_{p-1} is the skew-harmonic number defined by

$$H'_{p-1} := \sum_{j=1}^{p-1} \frac{(-1)^{j+1}}{j}.$$

Indeed, since $H_{p-1} \equiv 0 \pmod{p^2}$ by Wolstenholme's theorem, $H_{p-1} - H'_{p-1} = H_{\nu}$ provides $H'_{p-1} \equiv -H_{\nu} \pmod{p^2}$. So the assertion holds.

Lastly, we present an explicit expression of W_p, which is attributed to Beeger.

Proposition 2.6 (Beeger [10])**.** *We have*

$$W_p = \sum_{a=1}^{p-1}(-1)^a \binom{p-1}{a} q_p(a). \tag{2.10}$$

Proof. There are several ways for proving (2.10), but perhaps the simplest being to utilize an easy binomial functional identity such that

$$(1-e^t)^{p-1} = \sum_{a=0}^{p-1}(-1)^a \binom{p-1}{a} e^{at}.$$

Indeed, we differentiate both sides $p-1$ times with respect to t and set $t=0$. Then, the left-hand side yields

$$\frac{d^{p-1}}{dt^{p-1}}(1-e^t)^{p-1}\Big|_{t=0} = (p-1)!.$$

Further, using the obvious identity

$$\sum_{a=1}^{p-1}(-1)^a\binom{p-1}{a} = -1,$$

it follows that

$$(p-1)! = \sum_{a=1}^{p-1}(-1)^a\binom{p-1}{a}a^{p-1} = \sum_{a=1}^{p-1}(-1)^a\binom{p-1}{a}\left(a^{p-1}-1\right) - 1.$$

By moving the last term -1 to the most left side and dividing the whole by p, we can deduce (2.10). Note here that (2.10) provides Lerch's (2.1), since the congruence $(-1)^a\binom{p-1}{a} \equiv 1 \pmod{p}$ holds for $1 \le a \le p-1$. □

3. Application of a Miki-Type Linear Identity

In the author's previous work, the following linear identity for Bernoulli numbers involving two different kinds of sums was proved in an elementary way.

Theorem 3.1 (Agoh [4]). *For integers $n, m \ge 1$, we have*

$$\sum_{i=1}^{n-1} m^{n-i}\frac{B_i}{i} - \sum_{i=1}^{n-1}\binom{n}{i}m^{n-i}\frac{B_i}{i} = \sum_{j=1}^{m-1}\frac{(m-j)^n}{j} + m^n\left(H_n - H_m\right). \tag{3.1}$$

It should be noted that this identity embraces various properties of Bernoulli numbers, as we shall demonstrate below by some concrete examples.

(a) Identity (3.1) includes (1.1) as a special case. Indeed, by taking $m=1$ in (3.1), we get the simple formula

$$\sum_{i=1}^{n-1}\frac{B_i}{i} - \sum_{i=1}^{n-1}\binom{n}{i}\frac{B_i}{i} = H_n - 1. \tag{3.2}$$

Denote by $F(n)$ the left-hand side of (3.2). Using the easy identity $\left(\binom{n}{i} - \binom{n-1}{i}\right)\frac{1}{i} = \binom{n-1}{i-1}\frac{1}{i} = \frac{1}{n}\binom{n}{i}$ valid for $i \ge 1$, it follows that

$$F(n-1) - F(n) = -\frac{B_{n-1}}{n-1} + \sum_{i=1}^{n-2}\left(\binom{n}{i} - \binom{n-1}{i}\right)\frac{B_i}{i} + \binom{n}{n-1}\frac{B_{n-1}}{n-1}$$

$$= B_{n-1} + \frac{1}{n}\sum_{i=1}^{n-2}\binom{n}{i}B_i = -\frac{1}{n} \quad (n \geq 2),$$

which is exactly the same as the identity obtained by dividing both sides of (1.1) by n. Conversely, letting $F(1) := 0$, we have from the above,

$$F(n) = \sum_{k=2}^{n}(F(k) - F(k-1)) = \sum_{k=2}^{n}\frac{1}{k} = H_n - 1.$$

Therefore, it was shown that (3.2) is actually equivalent to (1.1).

(b) At first sight, it may appear as if (3.1) is entirely different from Faulhaber's formula (1.4); but surprisingly, they are equivalent. Such a very interesting fact was proved in [4, Theorem 2.2] by transforming (1.4) into the form

$$\sum_{i=1}^{n}\binom{n}{i-1}(k+1)^{n+1-i}\frac{B_i}{i} = \sum_{j=1}^{k+1}(k+1-j)^n - \frac{(k+1)^{n+1}}{n+1} \quad (k \geq 0),$$

and then by showing that this identity is effectively equivalent to (3.1).

(c) As has been also proved in [4, Theorem 2.3], taking $m = 1, 2, \ldots, p$ (with p an odd prime) in (3.1) and evaluating the sum of them modulo p^2, we are able to establish Miki's remarkable formula such that

$$\sum_{i=2}^{n-2}\frac{B_iB_{n-i}}{i(n-i)} - \sum_{i=2}^{n-2}\binom{n}{i}\frac{B_iB_{n-i}}{i(n-i)} = \frac{2H_nB_n}{n} \quad \text{(Miki [22])}, \tag{3.3}$$

valid for any $n \geq 4$. Miki himself proved this formula based on p-adic analysis and using the Fermat quotient. After a while, Gessel [16] gave a simple proof by applying properties of the Stirling number of the second kind. As can be obviously seen, (3.3) is constituted of two different kinds of convolution sums. For that reason, it would be safe to say that (3.1) is a linear version of Miki's (3.3).

By making use of (3.1), we first prove the following formulas involving both the Wilson and Fermat quotients. Note that these are not new (for instance, see Glaisher [17]). However, it seems that our proof relying on (3.1) is much simpler and easier to understand than the previously known proofs.

Theorem 3.2. *For an odd prime p and an integer $m \geq 1$ with $p \nmid m$, we have*

$$\begin{aligned} &\text{(i)} \quad \sum_{i=1}^{p-2}\frac{1}{m^i}\frac{B_i}{i} \equiv W_p + q_p(m) \pmod{p}; \\ &\text{(ii)} \quad \sum_{i=1}^{p-2}\frac{(-1)^i}{m^i}\frac{B_i}{i} \equiv W_p + q_p(m) + \frac{1}{m} \pmod{p}. \end{aligned} \tag{3.4}$$

In particular,

$$\begin{aligned} &\text{(iii)} \quad \sum_{i=1}^{p-2} \frac{B_i}{i} \equiv W_p \pmod{p}; \\ &\text{(iv)} \quad \sum_{i=1}^{p-2} (-1)^i \frac{B_i}{i} \equiv W_p + 1 \pmod{p}. \end{aligned} \tag{3.5}$$

Proof. Take $n = p$ in (3.1) and separate the terms involving B_{p-1} from the others. After cancelling common terms and dividing the whole by m, we get

$$\begin{aligned} &\sum_{i=1}^{p-2} \left(1 - \binom{p}{i}\right) m^{p-1-i} \frac{B_i}{i} + \left(1 - \binom{p}{p-1}\right) \frac{B_{p-1}}{p-1} \\ &\qquad = \frac{1}{m} \sum_{j=1}^{m-1} \frac{(m-j)^p}{j} + m^{p-1} \left(H_p - H_m\right). \end{aligned}$$

Let us denote by $Q_p(m)$ the special quotient defined by

$$Q_p(m) := \frac{pB_{p-1} + m^{p-1}}{p} = \frac{pB_{p-1} + 1}{p} + q_p(m) \in \mathbb{Z}_p.$$

Since $\binom{p}{i} \equiv 0 \pmod{p}$ $(i \neq 0, p)$, $H_{m-1} + \frac{1}{m} = H_m$, and $H_p = H_{p-1} + \frac{1}{p} \equiv \frac{1}{p} \pmod{p}$, it can be shown from Fermat's little theorem and (2.2) that

$$\begin{aligned} \sum_{i=1}^{p-2} \frac{1}{m^i} \frac{B_i}{i} &\equiv \left\{ \left(\binom{p}{p-1} - 1 \right) \frac{B_{p-1}}{p-1} + \frac{m^{p-1}}{p} \right\} + \frac{1}{m} \sum_{j=1}^{m-1} \left(\frac{m}{j} - 1 \right) - H_m \\ &\equiv \frac{pB_{p-1} + m^{p-1}}{p} + H_{m-1} - \frac{m-1}{m} - H_m \\ &\equiv Q_p(m) - 1 \equiv W_p + q_p(m) \pmod{p}, \end{aligned}$$

which is just (i). Meanwhile, (ii) is given immediately by replacing m with $p - m$ in (i) and using the fact that $q_p(p-m) \equiv q_p(m) + \frac{1}{m} \pmod{p}$. Note that (ii) is essentially the same as (i), because $B_1 = -\frac{1}{2}$ and $B_i = 0$ for all odd $i \geq 3$. The latter congruences (iii) and (iv) in (3.5) are nothing but the special cases of (3.4) (i) and (ii) for $m = 1$, respectively. □

By setting $m = 1$ in the above proof, we observe that

$$\sum_{i=1}^{p-2} \frac{B_i}{i} \equiv Q_p(1) - 1 \equiv B_{p-1} + \frac{1}{p} - 1 \pmod{p}.$$

So it can be concluded that (3.5) (iii) is essentially tantamount to (2.2).

Next, we denote by $H_n^{(i)}$ the generalized harmonic number of order $i \geq 1$, i.e.,

$$H_n^{(i)} := \sum_{k=1}^{n} \frac{1}{k^i} \quad (n \geq 1).$$

Thus, in particular, one has $H_n^{(1)} = H_n$.

Theorem 3.3. *For any fixed integer n with $1 \leq n \leq p-1$, we have*

$$\sum_{i=1}^{p-2} H_n^{(i)} \frac{B_i}{i} \equiv nW_p + q_p(n!) \pmod{p}. \tag{3.6}$$

Proof. We take $m = 1, 2, \ldots, n$ in (3.4) (i) and add up them all. Then, since $q_p(n!) \equiv \sum_{m=1}^{n} q_p(m) \pmod{p}$ by (1.6) (i), we can derive (3.6). □

The special case of (3.6) for $n = p-1$ turns out to Lerch's (2.1), because Faulhaber's formula (1.4) provides, for all $i = 1, 2, \ldots, p-2$,

$$H_{p-1}^{(i)} \equiv S_{p-1-i}(p-1) \equiv 0 \pmod{p}.$$

4. Discussion Based on Quadratic Residues and Non-Residues

In what follows, we assume that p is an odd prime with $p \equiv 1 \pmod 4$. Let R and S be the products of quadratic residues and non-residues modulo p in the interval $(0, p)$, respectively. Thus, using the Legendre symbol $(\frac{\cdot}{p})$, they are written as

$$R := \prod_{\substack{0<r<p \\ (\frac{r}{p})=1}} r \quad \text{and} \quad S := \prod_{\substack{0<s<p \\ (\frac{s}{p})=-1}} s.$$

Just to be sure, let us redefine $\nu := (p-1)/2$. Noting that $\left(\frac{k}{p}\right) = \left(\frac{p-k}{p}\right)$ is valid for all $k = 1, 2, \ldots, \nu$ when $p \equiv 1 \pmod 4$, we can get from Wilson's theorem,

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

Therefore, there exist the integers $U_p > 0$ and $V_p < 0$ satisfying

$$R + 1 = pU_p \quad \text{and} \quad S - 1 = -pV_p, \tag{4.1}$$

respectively. Since $(p-1)!$ can be written as

$$(p-1)! = RS = (-1 + pU_p)(1 - pV_p) = -1 + p\,(U_p + V_p) - p^2 U_p V_p,$$

by adding 1 to the whole and dividing by p, we obtain

$$W_p = \frac{RS+1}{p} \equiv U_p + V_p \equiv \frac{R-S+2}{p} \pmod{p}. \tag{4.2}$$

Furthermore, it can be derived from (4.1) that

$$\begin{aligned} &\text{(i)} \quad q_p(R) = \frac{1}{p}\left((-1+pU_p)^{p-1}-1\right) \equiv U_p \pmod{p}; \\ &\text{(ii)} \quad q_p(S) = \frac{1}{p}\left((1-pV_p)^{p-1}-1\right) \equiv V_p \pmod{p}. \end{aligned} \tag{4.3}$$

Thereby, the following congruence holds:

$$W_p \equiv U_p + V_p \equiv q_p(R) + q_p(S) \pmod{p}, \tag{4.4}$$

which is exactly the same as Lerch's (2.1) in view of (1.6) (i).

Based on (4.2) and (4.4), we are able to deduce some criteria for Wilson primes, as stated below.

Theorem 4.1. *A prime p with $p \equiv 1 \pmod 4$ is a Wilson prime if and only if each one of the following congruences holds:*

$$\begin{aligned} &\text{(i)} \quad RS+1 \equiv 0 \pmod{p^2}; \\ &\text{(ii)} \quad R-S+2 \equiv 0 \pmod{p^2}; \\ &\text{(iii)} \quad q_p(R)+q_p(S) \equiv 0 \pmod{p}. \end{aligned}$$

Next, let h be the class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$ and $\varepsilon := (t+u\sqrt{p})/2 > 1$ be the fundamental unit of this field. Hence, (t,u) is the least positive integer pair that satisfies the Pell equation $x^2 - py^2 = -4$. The most significant relationship between h and ε can be stated by the Dirichlet class number formula. That is to say,

$$h = \frac{\sqrt{p}}{2\log\varepsilon} L(1,\chi) \quad \text{(see, e.g., [28, Chap. 26])},$$

where $L(s,\chi)$ is the L-function attached to the Dirichlet character χ of conductor p, i.e., the Legendre symbol as it stands.

The following remarkable formula was first discovered by Kiselev [20], and later independently by Ankeny and Chowla [8]:

$$\frac{hu}{t} \equiv B_\nu \pmod{p}. \tag{4.5}$$

In their paper [7], Ankeny, Artin, and Chowla asked the question whether $p \nmid u$ is always true and this question came to be called the Ankeny-Artin-Chowla (AAC)

conjecture, which still remains unsolved. Since $h < \sqrt{p}$ (see, e.g., [24]); and so $p \nmid h$, we see from (4.5) that the AAC conjecture is tantamount to the question as to whether $B_\nu \not\equiv 0 \pmod{p}$ always holds.

Using traditional notation, let us write for an integer $n \geq 1$,

$$\varepsilon_n := \varepsilon^n = \left(\frac{t + u\sqrt{p}}{2}\right)^n = \frac{t_n + u_n\sqrt{p}}{2}; \tag{4.6}$$

thus, in particular, $t = t_1$ and $u = u_1$. Obviously, the pair (t_n, u_n) satisfies the same Pell equation as indicated above. The following congruence was initially announced by Ankeny, Artin, and Chowla in [6], and was later proved by Carlitz [12] (for a commentary on its surroundings, see [3]). Using the notation in (4.6), we have

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

Combining this with (4.5) and using (4.1), it follows that

$$\frac{R+S}{p} \equiv U_p - V_p \equiv 2B_\nu \pmod{p},$$

and hence, we obtain from (4.3) and (4.4) that

$$W_p \equiv 2(q_p(R) - B_\nu) \equiv 2(q_p(S) + B_\nu) \pmod{p},$$

which provides the criteria for Wilson primes as stated below.

Theorem 4.2. *A prime p with $p \equiv 1 \pmod 4$ is a Wilson prime if and only if each one of the following congruences holds:*

$$\begin{aligned} &\text{(i)} \quad q_p(R) - B_\nu \equiv 0 \pmod{p}; \\ &\text{(ii)} \quad a_p(S) + B_\nu \equiv 0 \pmod{p}. \end{aligned}$$

In what follows, we wish to rediscuss above R and S from a different perspective. Let g be a primitive root modulo p and g_i, $i \geq 0$, be the least positive residue of g^i modulo p. Thus, one has

$$g^i = g_i + p\left\lfloor \frac{g^i}{p} \right\rfloor, \quad 0 < g_i < p. \tag{4.7}$$

By expressing R and S by means of g, we obtain the following formula for W_p.

Theorem 4.3. *We have*

$$W_p \equiv \sum_{i=1}^{p-1} \frac{1}{g^i} \left\lfloor \frac{g^i}{p} \right\rfloor \pmod{p}. \tag{4.8}$$

Proof. In what follows, we denote

$$\alpha := \prod_{j=1}^{\nu} g^{2j} = g^{(p^2-1)/4} = g^{\nu(\nu+1)}; \quad \beta := \prod_{j=1}^{\nu} g^{2j-1} = g^{(p-1)^2/4} = g^{\nu^2}.$$

When $p \equiv 1 \pmod 4$, it is clear that $\nu + 1$ is odd and ν is even. Therefore, using the congruence $g^{\nu} \equiv -1 \pmod p$, we have

$$\alpha = (g^{\nu})^{\nu+1} \equiv -1 \pmod p; \quad \beta = (g^{\nu})^{\nu} \equiv 1 \pmod p. \tag{4.9}$$

For simplicity, put

$$X_p := \sum_{\substack{0<i<p \\ i \text{ even}}} \frac{1}{g^i} \left\lfloor \frac{g^i}{p} \right\rfloor \quad \text{and} \quad Y_p := \sum_{\substack{0<i<p \\ i \text{ odd}}} \frac{1}{g^i} \left\lfloor \frac{g^i}{p} \right\rfloor.$$

Using these notation and (4.9), it is possible to express R and S as follows:

$$\begin{aligned} \text{(i)} \quad R &= \prod_{\substack{0<i<p \\ i \text{ even}}} g_i = \prod_{\substack{0<i<p \\ i \text{ even}}} \left(g^i - p \left\lfloor \frac{g^i}{p} \right\rfloor \right) \\ &\equiv \alpha \left(1 - pX_p\right) \equiv \alpha + pX_p \pmod{p^2}; \\ \text{(ii)} \quad S &= \prod_{\substack{0<i<p \\ i \text{ odd}}} g_i = \prod_{\substack{0<i<p \\ i \text{ odd}}} \left(g^i - p \left\lfloor \frac{g^i}{p} \right\rfloor \right) \\ &\equiv \beta \left(1 - pY_p\right) \equiv \beta - pY_p \pmod{p^2}. \end{aligned} \tag{4.10}$$

Further, since $g^{\nu} \equiv -1 \pmod p$, we get $\prod_{i=1}^{p-1} g^i = (g^{\nu})^p \equiv -1 \pmod{p^2}$, which leads to

$$\alpha\beta = g^{\nu(\nu+1)+\nu^2} = g^{\nu p} \equiv -1 \pmod{p^2}.$$

Consequently, based on (4.9) and (4.10), we are able to express the product of R and S modulo p^2 in the form

$$\begin{aligned} RS &\equiv (\alpha + pX_p)(\beta - pY_p) \equiv \alpha\beta + p(\beta X_p - \alpha Y_p) \\ &\equiv -1 + p(X_p + Y_p) \pmod{p^2}. \end{aligned}$$

This congruence provides from (4.2) that

$$W_p \equiv \frac{RS+1}{p} \equiv X_p + Y_p \equiv \sum_{i=1}^{p-1} \frac{1}{g^i} \left\lfloor \frac{g^i}{p} \right\rfloor \pmod p,$$

and so the proof was complete. □

We proved (4.8) only in the case where $p \equiv 1 \pmod 4$, but it is also possible to verify in a similar way that (4.8) is also valid even if $p \equiv 3 \pmod 4$. For reference, see the proofs in [14, Theorem 2] and [5, Proposition 2.1].

Next we want to express B_ν appeared in (4.5) by means of g referring to the method as mentioned in [2].

Theorem 4.4. *We have*

$$2B_\nu \equiv \sum_{i=1}^{p-1} \frac{(-1)^i}{g^i} \left\lfloor \frac{g^i}{p} \right\rfloor - \frac{1}{2} q_p(g) \pmod p. \tag{4.11}$$

Proof. For an integer $n > 0$ we obtain from (4.7),

$$g^{in} = \left(g_i + p \left\lfloor \frac{g^i}{p} \right\rfloor \right)^n \equiv g_i^n + n g_i^{n-1} p \left\lfloor \frac{g^i}{p} \right\rfloor \pmod{p^2}.$$

Summing this up over $i = 1, 2, \ldots, p-1$ yields

$$\sum_{i=1}^{p-1} g^{in} \equiv \sum_{i=1}^{p-1} g_i^n + np \sum_{i=1}^{p-1} g_i^{n-1} \left\lfloor \frac{g^i}{p} \right\rfloor \pmod{p^2}. \tag{4.12}$$

Assuming that $p - 1 \nmid n$, the left-hand side of this can be written as

$$\begin{aligned} \sum_{i=1}^{p-1} g^{in} &= \frac{g^n(g^{n(p-1)} - 1)}{g^n - 1} = \frac{g^n((g^{p-1} - 1 + 1)^n - 1)}{g^n - 1} \\ &\equiv \frac{g^n}{g^n - 1} \left(\sum_{j=0}^{n} \binom{n}{j} (g^{p-1} - 1)^j - 1 \right) \\ &\equiv np \frac{g^n}{g^n - 1} q_p(g) \pmod{p^2}. \end{aligned}$$

On the other hand, based on the fact that $\{g_1, g_2, \ldots, g_{p-1}\} = \{1, 2, \ldots, p-1\}$, the first sum on the right-hand side of (4.12) can be written as, by using (1.4),

$$\sum_{i=1}^{p-1} g_i^n = S_n(p-1) \equiv pB_n \pmod{p^2}.$$

Subsequently, based on $g_i^{n-1} \equiv g^{i(n-1)} \pmod p$, let us replace the latter sum in (4.12) with $np \sum_{i=1}^{p-1} g^{i(n-1)} \lfloor g^i/p \rfloor$. As a result, assuming that $p \nmid n$ and dividing the whole by np, we are able to convert (4.12) into

$$\frac{g^n}{g^n - 1} q_p(g) \equiv \frac{B_n}{n} + \sum_{i=1}^{p-1} g^{i(n-1)} \left\lfloor \frac{g^i}{p} \right\rfloor \pmod p.$$

Take here $n = \nu$ and use $g^\nu \equiv -1 \pmod p$ to arrive at (4.11). □

We will close this section with stating the following two congruences for W_p, which are obtained from the addition and the subtraction of (4.8) and (4.11).

Corollary 4.5. *We have*

$$\text{(i)} \quad W_p \equiv -2B_\nu + 2\sum_{j=1}^{\nu} \frac{1}{g^{2j}} \left\lfloor \frac{g^{2j}}{p} \right\rfloor - \frac{1}{2}q_p(g) \pmod{p};$$

$$\text{(ii)} \quad W_p \equiv 2B_\nu + 2\sum_{j=1}^{\nu} \frac{1}{g^{2j-1}} \left\lfloor \frac{g^{2j-1}}{p} \right\rfloor + \frac{1}{2}q_p(g) \pmod{p}.$$

Of course, these congruences are valid only in the case where $p \equiv 1 \pmod 4$.

Acknowledgment. The author is thankful to the editor for helpful comments and suggestions that improved the presentation of the paper.

References

[1] T. Agoh, On Fermat and Wilson quotients, *Expo. Math.* **11** (1996), 145–170.

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

[3] T. Agoh, Congruences related to the Ankeny-Artin-Chowla conjecture, *Integers* **16** (2016), #A12, 30 pp.

[4] T. Agoh, On Miki's identity for Bernoulli numbers, *Integers* **16** (2016), #A73, 12 pp.

[5] T. Agoh, A note on the Wilson quotient, *Integers* **22** (2022), #A86, 10 pp.

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

[7] N. C. Ankeny, E. Artin, and S. Chowla, The class number of real quadratic fields, *Ann. of Math. (2)* **56** (1952), 479–493.

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

[9] 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.

[10] N. G. W. H. Beeger, On the congruence $(p-1)! \equiv -1 \pmod{p^2}$, *Mess. Math.* **49** (1920), 177–178.

[11] C. K. Caldwell, *The Prime Pages, The Prime Glossary: Wilson prime*, available online at https://primes.utm.edu/glossary/page.php?sort=WilsonPrime.

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

[13] E. Costa, R. Gerbicz, and D. Harvey, A search for Wilson primes, *Math. Comp.* **83** (2014), 3071–3091.

[14] R. Crandall, K. Dilcher, and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comput.* **66** (1997), 433–449.

[15] G. Eisenstein, Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definirt werden, Ber. über Verhandl. der Königl. *Preuß. Akad. Wiss. Berlin* **15** (1850) 36–42. Reprinted in *Mathematische Werke*, Vol. 2. 705–712, Chelsea, New York, 1975.

[16] I. M. Gessel, On Miki's identity for Bernoulli numbers, *J. Number Theory* **110** (2005), 75–82.

[17] J. W. L. Glaisher, On the residues of the sums of products of the first $p-1$ numbers and their powers, to modulus p^2 or p^3, *Quart. J. Math.* **31** (1899/1900), 321–353.

[18] J. W. L. Glaisher, On the residues of r^{p-1} to modulus p^p, p^3, etc., *Quart. J. Math.* **32** (1901), 1–27.

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

[20] 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.

[21] G. B. Mathews, *Theory of Numbers. Part 1.*, Cambridge, England: Deighton, Bell, Co., 1892.; 2nd ed, Chelsea Publishing Co., New York, 1961.

[22] H. Miki, A relation between Bernoulli numbers, *J. Number Theory* **10** (1978), 297–302.

[23] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math. (2)* **39** (1938), 350–360.

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

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

[26] OEIS Foundation Inc. (2020), The On-Line Encyclopedia of Integer Sequences, available online at http://oeis.org.

[27] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

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

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

[30] I. Sh. Slavutskii, About von Staudt congruences for Bernoulli numbers, *Comment. Math. Univ. St. Pauli* **48** (1999), 137–144.

[31] J. J. Sylvester, Sur une propriété des nombres premiers qui se ratache au théorème de Fermat, *C. R. Acad. Sci. Paris* **52** (1861), 161–163; Reprinted in *Sylvester's Collected Math. Papers*, Vol. 2, 229–231, Cambridge Univ. Press, 1908.