A NOTE ON THE WILSON QUOTIENT

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

Received: 5/23/22, Accepted: 8/19/22, Published: 9/12/22

Abstract

In this note, we first investigate relationships between some well-known formulas for the Wilson quotient. Subsequently, we discuss this quotient based on Eulerian numbers for establishing a new and original characterization of a Wilson prime by means of 'Eulerian quotients'.

1. Introduction

Wilson's theorem asserts that p is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$ holds. Based on this theorem the Wilson quotient W_p of p is defined by

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

If $W_p \equiv 0 \pmod{p}$, or equivalently, if $(p-1)! \equiv -1 \pmod{p^2}$, then p is called a *Wilson prime*. The known Wilson primes are only $5, 13$, and 563 (see A007540 in [15]) and it is still open whether there exist infinitely many such primes.

In our previous paper [3], we observed various types of formulas related to the Wilson quotient. Among them, one of the most important formulas is the following one attributed to Lerch in 1905. That is, it follows that for an odd prime p,

$$W_p \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p} \quad \text{(Lerch [13])}, \tag{1.1}$$

where $q_p(a)$ is the Fermat quotient with base a, $p \nmid a$, defined by

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

These quotients possess the logarithmic property. Precisely, for integers a, b with $p \nmid ab$ we have

$$\begin{aligned} &\text{(i)} \quad q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}; \\ &\text{(ii)} \quad q_p(a^n) \equiv n q_p(a) \pmod{p} \quad (n \geq 0). \end{aligned} \tag{1.2}$$

Both of them can be easily proved by direct calculation.

On the other hand, let B_n, $n = 0, 1, 2, \ldots$, be the Bernoulli numbers defined by the generating function

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

It is easy to find that $B_{2n+1} = 0$ and $(-1)^{n-1} B_{2n} > 0$ for all $n \geq 1$. As is widely known, the von Staudt-Clausen theorem asserts that

$$B_{2n} + \sum_{p-1|2n} \frac{1}{p} \in \mathbb{Z} \quad (n \geq 1), \tag{1.3}$$

where the sum is taken over all the primes p with $p - 1 \mid 2n$. So the denominator $D_{2n} > 0$ of B_{2n} can be explicitly represented by $D_{2n} = \prod_{p-1|2n} p$.

The most neat and concise formula involving both the Wilson quotient and the Bernoulli number is

$$W_p \equiv B_{p-1} + \frac{1}{p} - 1 \pmod{p} \quad \text{(Glaisher [8], Beeger [4])}. \tag{1.4}$$

As we have seen in many literature, this formula plays an important role as well as (1.1) in a study of more advanced properties of the Wilson quotient. A generalized version of (1.4) has been obtained by E. Lehmer [12] in 1938 by substantially proving that for any integer $m > 0$,

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

A brief summary of the development process of Fermat and Wilson quotients can be found, for instance, in [1].

This note is a continuation of the author's previous paper [3]. In Section 2 we investigate explicit relationships between some well-known formulas for the Wilson quotient. In Section 3, as a new approach, we discuss the Wilson quotient based on Eulerian numbers for establishing a new and original characterization of a Wilson prime by means of 'Eulerian quotients' (as defined in (3.4) below).

2. Equivalence Relations

As we have observed in [3, Proposition 2.2], Lerch's formula (1.1) has a direct relationship with (1.4) and it can be shown that they are actually equivalent to each other. Following this example, in this section we would like to search for equivalence relationships between several other known formulas for W_p by having (1.1) and (1.4) participate.

In what follows, let g be a primitive root modulo p and g_i be the least positive residue of g^i $(i \geq 0)$ modulo p; so that we have

$$g^i = g_i + p\left\lfloor \frac{g^i}{p} \right\rfloor, \quad 0 < g_i < p. \tag{2.1}$$

For brevity we now denote

$$A_p := \frac{g^{p(p-1)/2}+1}{p}, \quad \alpha_p := \sum_{i=1}^{p-1} \frac{1}{g^i}\left\lfloor \frac{g^i}{p} \right\rfloor,$$
$$\text{and} \quad \beta_p := \sum_{1\leq i<j\leq p-1} \frac{1}{g^{i+j}}\left\lfloor \frac{g^i}{p} \right\rfloor \left\lfloor \frac{g^j}{p} \right\rfloor.$$

To begin with, we introduce the following congruences related to the quotient W_p. Subsequently, we wish to prove that one of which is equivalent to Lerch's formula (1.1) (Proposition 2.2 below).

Proposition 2.1. *For an odd prime p we have*

$$W_p \equiv A_p + \alpha_p - p\beta_p \pmod{p^2}. \tag{2.2}$$

In particular,

$$W_p \equiv \alpha_p \pmod{p} \quad \text{(cf. [7, Theorem 2] and [3, Proposition 4.3])}. \tag{2.3}$$

Proof. First note that $\prod_{i=1}^{p-1} g^i = g^{p(p-1)/2}$. Since $g^{(p-1)/2} \equiv -1 \pmod{p}$, we have $g^{p(p-1)/2} \equiv -1 \pmod{p^2}$; and thus, $p \mid A_p$. Using (2.1), it is shown that

$$\begin{aligned}(p-1)! = \prod_{i=1}^{p-1} g_i &= \prod_{i=1}^{p-1}\left(g^i - p\left\lfloor \frac{g^i}{p} \right\rfloor\right)\\ &\equiv g^{p(p-1)/2}\left(1 - p\alpha_p + p^2\beta_p\right) \pmod{p^3}.\end{aligned}$$

Adding 1 to both sides and then dividing throughout by p, we get

$$W_p \equiv A_p - g^{p(p-1)/2}\left(\alpha_p - p\beta_p\right) \equiv A_p + \alpha_p - p\beta_p \pmod{p^2},$$

which is just (2.2) as desired. The latter congruence follows immediately from (2.2) in view of $p \mid A_p$. □

According to the multinomial identity

$$\left(\sum_{i=1}^{n} x_i\right)^2 - 2\sum_{0\leq i<j\leq n} x_i x_j = \sum_{i=1}^{n} x_i^2 \quad (n \geq 2),$$

we may rewrite β_p, if necessary, as

$$\beta_p = \frac{1}{2}\left\{\left(\sum_{i=1}^{p-1}\frac{1}{g^i}\left\lfloor\frac{g^i}{p}\right\rfloor\right)^2 - \sum_{i=1}^{p-1}\left(\frac{1}{g^i}\left\lfloor\frac{g^i}{p}\right\rfloor\right)^2\right\} = \frac{1}{2}\alpha_p^2 - \frac{1}{2}\sum_{i=1}^{p-1}\frac{1}{g^{2i}}\left\lfloor\frac{g^i}{p}\right\rfloor^2.$$

Next, we prove the following statement by examining an explicit relationship between α_p and the sum of Fermat quotients.

Proposition 2.2. *Formula* (2.3) *is equivalent to Lerch's formula* (1.1).

Proof. As is obvious, we have

$$\sum_{a=1}^{p-1} q_p(a) = \sum_{i=1}^{p-1} q_p(g_i) = \frac{1}{p}\left(\sum_{i=1}^{p-1} g_i^{p-1} - (p-1)\right).$$

Using (2.1), the sum on the most right-hand side can be written as follows:

$$\begin{aligned}\sum_{i=1}^{p-1} g_i^{p-1} &= \sum_{i=1}^{p-1}\left(g^i - p\left\lfloor\frac{g^i}{p}\right\rfloor\right)^{p-1} \\ &= \sum_{i=1}^{p-1}\sum_{k=0}^{p-1}(-1)^{p-1-k}\binom{p-1}{k}g^{ik}\left(p\left\lfloor\frac{g^i}{p}\right\rfloor\right)^{p-1-k} \\ &\equiv \sum_{i=1}^{p-1} g^{i(p-1)} + p\sum_{i=1}^{p-1} g^{i(p-2)}\left\lfloor\frac{g^i}{p}\right\rfloor \pmod{p^2}.\end{aligned} \tag{2.4}$$

We now observe individually two sums on the last side of (2.4). Using Fermat's little theorem and the fact that $p \mid \binom{p}{a}$ unless $a = 0$ and p, the first sum can be simplified as

$$\begin{aligned}\sum_{i=1}^{p-1} g^{i(p-1)} &= \frac{g^{p(p-1)} - g^{p-1}}{g^{p-1}-1} = \frac{((g^{p-1}-1)+1)^p - g^{p-1}}{g^{p-1}-1} \\ &= \sum_{a=1}^{p}\binom{p}{a}\left(g^{p-1}-1\right)^{a-1} - 1 \equiv p-1 \pmod{p^2}.\end{aligned}$$

Meanwhile, since $g^{i(p-2)} \equiv \frac{1}{g^i} \pmod{p}$, the latter sum is written as p times the whole of

$$\sum_{i=1}^{p-1} g^{i(p-2)}\left\lfloor\frac{g^i}{p}\right\rfloor \equiv \sum_{i=1}^{p-1}\frac{1}{g^i}\left\lfloor\frac{g^i}{p}\right\rfloor \equiv \alpha_p \pmod{p}.$$

Substitute these congruences into (2.4) and then subtract $p-1$ from the whole. After dividing both sides by p, we finally obtain

$$\sum_{i=1}^{p-1} q_p(g_i) \equiv \alpha_p \equiv W_p \pmod{p},$$

which verifies the statement. □

The Faulhaber formula concerning the sum of the nth power of the first k positive integers states that

$$S_n(k) := \sum_{m=1}^{k} m^n = \sum_{i=1}^{n+1} \frac{1}{i} \binom{n}{i-1} (k+1)^i B_{n+1-i}. \tag{2.5}$$

We shall make use of this formula to prove the following statement.

Proposition 2.3. *Formula* (2.3) *is equivalent to* (1.4).

Proof. When $p = 3$, putting $g = 2$, we have $\alpha_3 = \frac{1}{4}$ and $B_2 + \frac{1}{3} - 1 = -\frac{1}{2}$. Since $\frac{1}{4} \equiv -\frac{1}{2} \pmod 3$, the statement holds true for $p = 3$. Next assume that $p \geq 5$. Since $\{g_i \mid 1 \leq i \leq p-1\} = \{1, 2, \ldots, p-1\}$, taking $n = k = p-1$ in (2.5), it is shown that

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

On the other hand, using (2.1) and Fermat's little theorem, we have

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

Equating these and dividing both sides by p, we finally obtain

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

so the proof was complete. □

Proposition 2.4. *Formula* (1.4) *is equivalent to the congruence*

$$W_p \equiv \sum_{i=1}^{p-2} \frac{B_i}{i} \pmod p \quad \text{(cf., e.g., [8] and [3, (3.5)])}. \tag{2.6}$$

Proof. As a Miki-type linear recurrence relation involving two different kinds of sums for divided Bernoulli numbers, it is known that

$$\sum_{i=1}^{n-1}\frac{B_i}{i}-\sum_{i=1}^{n-1}\binom{n}{i}\frac{B_i}{i}=H_n-1\quad\text{(see, e.g., [2, Corollary 3.3])},\tag{2.7}$$

where H_n is the nth harmonic number, namely

$$H_0:=0,\quad H_n:=1+\frac{1}{2}+\cdots+\frac{1}{n}\quad(n\geq 1).$$

We take here $n=p$ and gather the terms involving B_{p-1} in one place. Since $p\mid\binom{p}{i}$ $(i\neq 0,p)$ and $H_p=H_{p-1}+\frac{1}{p}\equiv\frac{1}{p}\pmod p$ by Wolstenholme's theorem, we can deduce the congruence

$$\sum_{i=1}^{p-1}\frac{B_i}{i}-\sum_{i=1}^{p-1}\binom{p}{i}\frac{B_i}{i}\equiv\sum_{i=1}^{p-2}\frac{B_i}{i}-B_{p-1}\equiv\frac{1}{p}-1\pmod p,$$

and this verifies the statement. □

Note that (2.6) is the special case for $m=1$ of the more general congruence

$$W_p\equiv\sum_{i=1}^{p-2}\frac{1}{m^i}\frac{B_i}{i}-q_p(m)\pmod p\quad\text{(Glaisher [8])},$$

valid for any integer $m\geq 1$ with $p\nmid m$. A simple and concise proof of this formula has been given in [3, Section 3] by applying a general form of (2.7), namely

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

3. A New Approach Based on Eulerian Numbers

For any given permutation σ on $\{1,2,\ldots,n\}$, an ascent of σ is an index i with $1\leq i<n$ such that $\sigma(i)<\sigma(i+1)$. The *Eulerian number* $A(n,k)$ is the number of permutations with k ascents. These numbers appear in the so-called Worpitzky identity (cf. [16] and [6])

$$x^n=\sum_{k=0}^{n}\binom{x+n-k}{n}A(n,k)\quad(n\geq 0),$$

and $A(n,k)$ can be expressed explicitly in the form

$$A(n,k)=\sum_{i=0}^{k}(-1)^i\binom{n+1}{i}(k-i)^n\quad(0\leq k\leq n).\tag{3.1}$$

It is also commonly known that

$$A(n,k)=\sum_{i=1}^{k}(-1)^{k-i}i!S(n,i)\binom{n-i}{k-i}\quad(1\le k\le n),$$

where $S(n,m)$ is the Stirling number of the second kind. So we may, of course, use these formulas as the definition of the Eulerian numbers.

Assuming that $A(0,0)=1$, $A(n,0)=1$ for $n\ge 1$, and $A(n,k)=0$ if $n<k$ by convention, it is easy to observe that they satisfy the recurrence relations

$$\begin{aligned}&\text{(i)}\quad A(n,k)=A(n,n+1-k);\\&\text{(ii)}\quad A(n+1,k)=kA(n,k)+(n+2-k)A(n,k-1).\end{aligned}\tag{3.2}$$

For much more advanced properties of these numbers, see, e.g., [5, 9–11, 14].

As is obvious, the sum of Eulerian numbers for any fixed n is the total number of permutations of the numbers 1 to n, i.e., the order of the symmetric group S_n. So that we have

$$\sum_{k=1}^{n}A(n,k)=n!\quad(n\ge 1).$$

Setting here $n=p-1$ for an odd prime p leads to the identity

$$\sum_{k=1}^{p-1}A(p-1,k)=(p-1)!.$$

Using (3.1) and the fact that $p\mid\binom{p}{i}$ unless $i=0,p$, each term on the left-hand side of the above identity can be evaluated modulo p^2 as follows:

$$\begin{aligned}A(p-1,k)&=\sum_{i=0}^{k-1}(-1)^i\binom{p}{i}(k-i)^{p-1}\\&=\sum_{i=0}^{k-1}(-1)^ip\binom{p}{i}\frac{(k-i)^{p-1}-1}{p}+\sum_{i=0}^{k-1}(-1)^i\binom{p}{i}\\&=\sum_{i=0}^{k-1}(-1)^ip\binom{p}{i}q_p(k-i)+\sum_{i=0}^{k-1}(-1)^i\binom{p}{i}\\&=(-1)^k\sum_{j=1}^{k}(-1)^jp\binom{p}{k-j}q_p(j)+\sum_{i=0}^{k-1}(-1)^i\binom{p}{i}\\&\equiv pq_p(k)+1+\sum_{i=1}^{k-1}(-1)^i\binom{p}{i}\pmod{p^2}.\end{aligned}$$

Noting that $\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1} \equiv (-1)^{i-1}\frac{p}{i} \pmod{p^2}$ for $i \geq 1$ and dividing throughout by p, we can deduce the congruence

$$\begin{aligned} q_p(k) &\equiv \frac{1}{p}\left(A(p-1,k) - 1 - \sum_{i=1}^{k-1}(-1)^i\binom{p}{i}\right) \\ &\equiv \Phi_p(k) + H_{k-1} \pmod{p}, \end{aligned} \tag{3.3}$$

where $\Phi_p(k)$ is the special quotient defined by

$$\Phi_p(k) := \frac{A(p-1,k)-1}{p} \in \mathbb{Z}, \quad k \geq 1. \tag{3.4}$$

It is not for sure whether such the quotient has been dealt with in the past literature, but let us call it for now the *Eulerian quotient of* p associated with $k \geq 1$. It is obvious from (3.2) (i) that $\Phi_p(1) = \Phi_p(p-1) = 0$ and

$$\Phi_p(k) = \Phi_p(p-k), \quad k = 2, 3, \ldots, \frac{p-1}{2}$$

hold. Furthermore, we see that (3.2) (ii) provides

$$k\Phi_p(k) + (p+1-k)\Phi_p(k-1) = \frac{A(p,k)-p-1}{p} \quad (2 \leq k \leq p-1).$$

Making use of (3.3), we are able to establish the following formula.

Theorem 3.1. *For an odd prime $p \geq 5$ we have*

$$W_p \equiv 2\sum_{k=1}^{(p-1)/2}\Phi_p(k) + 1 \pmod{p}. \tag{3.5}$$

Proof. Since the harmonic numbers satisfy the recurrence relation

$$\sum_{k=0}^{n} H_k = (n+1)H_n - n,$$

summing up $\Phi_p(k)$ over $k = 1, 2, \ldots, p-1$, we obtain from (1.1) and (3.3) that

$$\begin{aligned} W_p &\equiv \sum_{k=1}^{p-1} q_p(k) \equiv \sum_{k=1}^{p-1}(\Phi_p(k) + H_{k-1}) \\ &\equiv \sum_{k=1}^{p-1}\Phi_p(k) + (p-1)H_{p-2} - (p-2) \\ &\equiv 2\sum_{k=1}^{(p-1)/2}\Phi_p(k) + 1 \pmod{p}, \end{aligned}$$

as desired. □

For example. if $p = 11$, then we have (cf. A008292 in [15])

$$A(10,1) = 1; \quad A(10,2) = 1013; \quad A(10,3) = 147840;$$
$$A(10,4) = 1455192; \quad A(10,5) = 11310354.$$

Thus, the Eulerian quotients corresponding to these are given by

$$\Phi_{11}(1) \equiv 0; \quad \Phi_{11}(2) = 92 \equiv 4; \quad \Phi_{11}(3) = 4349 \equiv 4;$$
$$\Phi_{11}(4) = 41381 \equiv 10; \quad \Phi_{11}(5) = 119123 \equiv 4 \pmod{11},$$

respectively. So the right-hand side of (3.5) for $p = 11$ can be evaluated as

$$2\sum_{k=1}^{5} \Phi_{11}(k) + 1 \equiv 2(4 + 4 + 10 + 4) + 1 \equiv 1 \pmod{11},$$

which is consistent with $W_{11} = 329891 \equiv 1 \pmod{11}$ (cf. A007619 in [15]).

The following corollary is an immediate consequence of (3.5).

Corollary 3.2. *A prime $p \geq 5$ is a Wilson prime if and only if the congruence*

$$\sum_{k=1}^{(p-1)/2} \Phi_p(k) \equiv \frac{p-1}{2} \pmod{p} \tag{3.6}$$

holds.

It seems, as far as we know, that congruence (3.6) involving the sum of Eulerian quotients is new and original as one of the characterizations of a Wilson prime.

Acknowledgement. The author is thankful to the anonymous referee for carefully reviewing the first version of this note. Furthermore, the author thanks the editor for providing meaningful feedback.

References

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

[2] T. Agoh, Linear recurrences for Bernoulli polynomials involving different kinds of sums, *Integers* **21** (2021), #A73, 12 pp.

[3] T. Agoh, Congruences related to the Wilson quotient, preprint.

[4] 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** (1913/1914), 72–85.

[5] P. L. Butzer and M. Hauss, Eulerian numbers with fractional order parameters. *Aequationes Math.* **46** (1993), 119–142.

[6] L. Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, rev. enl. ed. Dordrecht, Netherlands: Reidel, 1974.

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

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

[9] H. W. Gould, Evaluation of sums of convolved powers using Stirling and Eulerian numbers, *Fibonacci Quart.* **16** (1978), 488–497.

[10] L. C. Hsu and P. J.-S. Shiue, On certain summation problems and generalizations of Eulerian polynomials and numbers, *Discrete Math.* **204** (1999), 237–247.

[11] M. V. Koutras, Eulerian numbers associated with sequences of polynomials, *Fibonacci Quart.* **32** (1994), 44–57.

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

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

[14] L. Lesieur and J.-L. Nicolas, On the Eulerian numbers $M_n = \max_{1\leq k\leq n} A(n,k)$, *European J. Combin.* **13** (1992), 379–399.

[15] N. J. A. Sloane, ed., The Online Encyclopedia of Integer Sequences (OEIS). Available at http://oeis.org/.

[16] J. Worpitzky, Studien über die Bernoullischen und Eulerischen Zahlen, *J. Reine Angew. Math.* **94** (1883), 203–232.