A CHARACTERIZATION OF WILSON-LERCH PRIMES

John Blythe Dobson
1170 Spruce Street, Winnipeg, Manitoba, Canada
johnblythedobson@gmail.com

Received: 11/22/15, Revised: 3/28/16, Accepted: 6/18/16, Published: 7/22/16

Abstract

This note presents criteria in terms of Bernoulli numbers for a prime to be simultaneously a Wilson prime and a Lerch prime.

1. Introduction

Many kinds of special primes can be characterized by the fact that they satisfy a congruence modulo p^2 which is only satisfied modulo p by other primes. For example, the Wieferich primes ([11, A001220]) are defined by $2^{p-1} \equiv 1 \pmod{p^2}$, and the Mirimanoff primes ([11, A014127]) by $3^{p-1} \equiv 1 \pmod{p^2}$, these being the best-known examples of the vanishing of the Fermat quotient $q_p(a) = (a^{p-1} - 1)/p$ modulo p. Or more generally, special primes may satisfy a congruence modulo p^n which is only satisfied modulo p^{n-1} by other primes; for example, the Wolstenholme primes ([11, A088164]) are defined by $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$.

In a similar manner, a Wilson prime ([11, A007540]) is classically defined by the condition that p divides its Wilson quotient $W_p = (\{p-1\}! + 1)/p$; i. e. $(p-1)! \equiv -1 \pmod{p^2}$, and a Lerch prime ([11, A197632]) by the condition that p divides its Lerch quotient (see below); i. e. $\sum_{a=1}^{p-1} q_p(a) \equiv W_p \pmod{p^2}$. The Wilson primes $< 2 \cdot 10^{13}$ are 5, 13, and 563 ([3], [4]), and the Lerch primes $< 4,496,113$ are 3, 103, 839, and 2237 [13], with no overlap between the two sequences in the ranges examined. In this note, we present analogous criteria for a prime to possess both of these properties simultaneously. We do not presume that our criteria have anything new to offer from a computational perspective; and considering that the search for Wilson primes has already been carried nearly to the limits of existing means of computation, it is doubtful whether any actual example could be discovered in the foreseeable future. Nonetheless, we present our results in the hope that they may shed some light on the theoretical possibility, or impossibility, of a Wilson-Lerch prime.

2. The Wilson Quotient

The fundamental definition of the Wilson quotient is $W_p = (\{p-1\}! + 1)/p$. In 1899, Glaisher [5] proved that (in the modern notation for the Bernoulli numbers, with $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_3 = B_5 = B_7 = \cdots = 0$, etc.),

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

and generalizations of this will be found in [9], [16], and [2]. Because W_p is an integer for all primes, the right-hand side is p-integral, meaning that when written as a reduced fraction, the denominator is not divisible by p. Thus the right-hand side has a p-adic valuation of at least 0, or equivalently,

$$B_{p-1} - 1 + \frac{1}{p} \equiv 0 \pmod{p^0}. \tag{2}$$

Clearly the Wilson primes are distinguished by the stricter congruence

$$B_{p-1} - 1 + \frac{1}{p} \equiv 0 \pmod{p}. \tag{3}$$

Now Kummer's congruence for the Bernoulli numbers, as extended by Johnson [7] to the case where $p-1$ divides the index, gives

$$\frac{B_{m(p-1)} - 1 + \frac{1}{p}}{m(p-1)} \equiv \frac{B_{p-1} - 1 + \frac{1}{p}}{p-1} \pmod{p} \quad (p > 2),$$

where m may be any positive integer, even a multiple of $p-1$ or of p. Since we do not require this theorem in its full generality, for the sake of simplicity we rewrite it with $m = 2$:

$$\frac{B_{2p-2} - 1 + \frac{1}{p}}{2p-2} \equiv \frac{B_{p-1} - 1 + \frac{1}{p}}{p-1} \pmod{p} \quad (p > 2). \tag{4}$$

Multiplying throughout by $2(p-1)$, and using (1), we obtain

$$\begin{aligned} B_{2p-2} - 1 + \frac{1}{p} &\equiv 2\left\{B_{p-1} - 1 + \frac{1}{p}\right\} \\ &\equiv B_{p-1} - 1 + \frac{1}{p} + W_p \pmod{p}; \end{aligned}$$

in other words,

$$W_p \equiv B_{2p-2} - B_{p-1} \pmod{p}. \tag{5}$$

This is a well-known result of E. Lehmer [9], but we think the derivation from Johnson's supplement to Kummer's congruence is illuminating. For a Wilson prime, clearly we thus have

$$B_{2p-2} \equiv B_{p-1} \pmod{p}. \tag{6}$$

While at first glance this may appear to be a pointless reformulation of (3), the usefulness of this expression will become apparent below. We will also make use of a result of Slavutskii, who rediscovered Johnson's result (4) and extended it to obtain several theorems connecting three Bernoulli numbers with indices divisible by $p-1$, including the following [12]:

$$B_{3p-3} \equiv 3B_{2p-2} - 3B_{p-1} + 1 - \frac{1}{p} \pmod{p^2}. \tag{7}$$

At the risk of belaboring the obvious, we point out that this implies for all primes

$$B_{3p-3} - 1 + \frac{1}{p} \equiv 0 \pmod{p^0}, \tag{8}$$

and likewise a condition for the Wilson primes equivalent to (6) and analogous in form to (3),

$$B_{3p-3} - 1 + \frac{1}{p} \equiv 0 \pmod{p}. \tag{9}$$

These congruences may be compared with Theorem 2 below.

3. The Lerch quotient

In 1905, Lerch [10] proved that

$$\sum_{a=1}^{p-1} q_p(a) \equiv W_p \pmod{p} \quad (p > 2). \tag{10}$$

In homage to this important congruence, Jonathan Sondow [13] defined the Lerch quotient,

$$\ell_p = \frac{\sum_{a=1}^{p-1} q_p(a) - W_p}{p},$$

and a Lerch prime as one that divides this quotient; in other words, a prime for which

$$\sum_{a=1}^{p-1} q_p(a) \equiv W_p \pmod{p^2}. \tag{11}$$

In a 1953 paper by Carlitz [2], (1) and (10) are combined and partly strengthened to give

$$\sum_{a=1}^{p-1} q_p(a) \equiv B_{p-1} - 1 + \frac{1}{p} \pmod{p^2} \quad (p > 3). \tag{12}$$

This supplies an alternate criterion for a Lerch prime, as one satisfying the congruence

$$W_p \equiv B_{p-1} - 1 + \frac{1}{p} \pmod{p^2}, \tag{13}$$

which appears in a slightly different notation in Sondow. It will be noted that (13) bears the same relation to (1) as (12) bears to (10); i. e. each is a p^2 variant on a congruence satisfied by all primes. As we shall see below, the closed form (13) crucially facilitates the comparison of Lerch primes with Wilson primes.

Incidentally, evaluating the left-hand side of (12) when the modulus is a higher power of p is a straightforward task, for by the Euler-MacLaurin summation formula, its value is given exactly by

$$\sum_{a=1}^{p-1} q_p(a) = -1 + \frac{1}{p} + \sum_{j=1}^{p} \binom{p}{j} p^{j-2} B_{p-j} \quad (p > 3), \tag{14}$$

where B_{p-j} vanishes for all even j except $j = p - 1$. This identity, in which the sum in the right-hand side is really just the usual expansion of $\frac{1}{p^2}\{B_p(p) - B_p\}$ with the terms reversed, can be used to obtain congruences like (12) to any desired precision, though (12) is sufficient for our purpose.

4. Connecting the Wilson Quotient with the Lerch Quotient

The Wilson quotient is likewise defined by an identity, which — as pointed out by Lehmer [8] — traces back to Euler and appears in an independent proof of (10) given by Beeger [1]:

$$\begin{aligned} W_p &= \frac{1}{p} \cdot \sum_{a=1}^{p-1} (-1)^a \binom{p-1}{a} \left(a^{p-1} - 1\right) \\ &= \sum_{a=1}^{p-1} (-1)^a \binom{p-1}{a} q_p(a). \end{aligned} \tag{15}$$

The final step of Beeger's proof depends on the well-known result of Lucas (1879) that $\binom{p-1}{a} \equiv (-1)^a \pmod{p}$ for all a such that $1 \le a \le p-1$. The evaluation of the right-hand side of (15) when the modulus is a higher power of p appears to be in general a much more difficult problem. However, as a starting point we can apply the refinement of Lucas's result by Lehmer [9], which states:

$$\binom{p-1}{a} \equiv (-1)^a \left\{1 - pH_a + \frac{p^2}{2}H_a^2 - \frac{p^2}{2}H_{a,2}\right\} \pmod{p^3}, \tag{16}$$

where H_a is the harmonic number $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{a}$, and $H_{a,2}$ is the generalized harmonic number $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{a^2}$. This result, which in its essence can be traced back to Glaisher [6], and which has been extended to the modulus p^4 by Z. H. Sun [15], may be combined with (15) to give the following refinement of Lerch's congruence (10):

$$W_p \equiv \sum_{a=1}^{p-1} q_p(a) - p \cdot \sum_{a=1}^{p-1} H_a\, q_p(a) + \frac{p^2}{2} \cdot \sum_{a=1}^{p-1} H_a^2\, q_p(a) - \frac{p^2}{2} \cdot \sum_{a=1}^{p-1} H_{a,2}\, q_p(a) \pmod{p^3}. \tag{17}$$

So long as $a \leq p-1$, it is obvious that H_a and $H_{a,2}$ are p-integral, and so must be the sums containing them. We may thus deduce directly from (16) the weaker

$$\binom{p-1}{a} \equiv (-1)^a \{1 - pH_a\} \pmod{p^2}, \tag{18}$$

and directly from (17) the weaker

$$W_p \equiv \sum_{a=1}^{p-1} q_p(a) - p \cdot \sum_{a=1}^{p-1} H_a\, q_p(a) \pmod{p^2}. \tag{19}$$

The sums of products of harmonic numbers and Fermat quotients in (17) are relatively intractable, but having recourse to an evaluation of the Wilson quotient by Sun [14], which was obtained by a quite different method, it is known that

$$W_p \equiv \frac{1}{p} - \frac{B_{p-1}}{p-1} + \frac{B_{2p-2}}{2p-2} - \frac{p}{2}\left(\frac{B_{p-1}}{p-1}\right)^2 \pmod{p^2} \quad (p > 3), \tag{20}$$

where the sum of the first two terms in the right-hand side is congruent to $W_p \pmod{p}$, and the sum of the last two terms is a multiple of p. This result, incidentally, establishes that the mod p^2 evaluation of the sum in (12) in terms of a Bernoulli number has no such simple counterpart in terms of the Wilson quotient. It also allows us to state:

Lemma 1. *A Lerch prime $p > 3$ is characterized by the congruence*

$$W_p \equiv \frac{B_{2p-2}}{2p} - \frac{B_{p-1}^2}{2p-2} \pmod{p}. \tag{21}$$

Proof. Sun's mod p^2 congruence for the Wilson quotient (20) may be combined with the definition of a Lerch prime based on Carlitz's congruence (13) to give another sufficient condition for a Lerch prime > 3:

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

which upon multiplication throughout by $(p-1)/p$ and the cancellation of like terms gives

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

Glaisher's congruence (1) states that $W_p \equiv B_{p-1} - 1 + \frac{1}{p} \pmod{p}$, hence the result follows. □

We can now give a first condition for a Wilson prime to be a Lerch prime:

Theorem 1. *A prime $p > 3$ is simultaneously a Wilson prime and a Lerch prime if it satisfies the congruence*

$$B_{2p-2} \equiv B_{p-1} \pmod{p^2}. \tag{22}$$

Proof. Setting the left-hand side of (21) to 0 and multiplying throughout by $2p(p-1)$ gives

$$(p-1) \cdot B_{2p-2} \equiv p \cdot B_{p-1}^2 \pmod{p^2}.$$

Substituting the definition of a Wilson prime (3) in the form $p \cdot B_{p-1} \equiv p - 1 \pmod{p^2}$ into the right-hand side of the above gives

$$(p-1) \cdot B_{2p-2} \equiv (p-1) \cdot B_{p-1} \pmod{p^2},$$

and cancelling the common term $p - 1$, the result follows. □

Finally, (22) can be rewritten using only a single Bernoulli number, thus giving a second condition for a Wilson prime to be a Lerch prime:

Theorem 2. *A prime $p > 3$ is simultaneously a Wilson prime and a Lerch prime if it satisfies the congruence*

$$B_{3p-3} - 1 + \frac{1}{p} \equiv 0 \pmod{p^2}. \tag{23}$$

Proof. Apply the condition (22) to Slavutskii's congruence (7). □

To summarize, we note that the three congruences (4), (6), and (22), may be seen as forming a progression of increasing stringency, with (4) characterizing primes in general, (6) the Wilson primes, and (22) the Wilson-Lerch primes. The first, though fundamental, has not been traced earlier than Johnson's paper of 1975 [7], the second has not been traced earlier than Lehmer's paper of 1938 [9], and the third, at least in regard to the interpretation given to it herein, is believed to be new.

Finally, an example of a progression of congruences where the only notational change is the escalation of the power of p in the modulus may be seen in (8), (9), and (23), which characterize the primes, the Wilson primes, and the Wilson-Lerch primes, respectively.

Acknowledgements I am grateful to Jonathan Sondow, and to the anonymous referee, for valuable suggestions as to the improvement of the presentation.

References

[1] N. G. W. H. Beeger. Quelques remarques sur les congruences $r^{p-1} \equiv 1 \mod p^2$ et $(p-1)! \equiv -1 \mod p^2$, *Messenger of Math.* **43** (1913–1914), 72–84.

[2] L. Carlitz. Some congruences for the Bernoulli numbers, *Amer. J. Math.* **75** (1953), 163–172.

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

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

[5] 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, *Q. J. Math.* **31** (1899–1900), 321–353.

[6] J. W. L. Glaisher. Residues of binomial-theorem coefficients with respect to p^3, *Q. J. Math.* **31** (1899–1900), 110–124.

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

[8] E. Lehmer. A note on Wilson's quotient, *Amer. Math. Monthly* **44** (1937), 237–238.

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

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

[11] The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org.

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

[13] J. Sondow. Lerch quotients, Lerch primes, Fermat-Wilson quotients, and the Wieferich-non-Wilson primes 2, 3, 14771, in M. B. Nathanson (ed.), *Combinatorial and Additive Number Theory*, Springer Proc. Math. Stat. **101** (2014), 243–255.

[14] Z.-H. Sun. Congruences concerning Bernoulli numbers and Bernoulli polynomials, *Discrete Appl. Math.* **105** (2000), 193–223.

[15] Z.-H. Sun. Congruences involving Bernoulli and Euler numbers, *J. Number Theory* **128** (2008), 280–312.

[16] H. S. Vandiver. Simple explicit expressions for generalized Bernoulli numbers of the first order, *Duke Math. J.* **8** (1941), 575–584.