# A note on Lerch primes

John Blythe Dobson (j.dobson@uwinnipeg.ca)

March 24, 2014

## Contents

**Abstract**

This note presents two alternate criteria for the Lerch primes, and discusses the question of whether a number can be simultaneously a Lerch prime and a Wilson prime.
*Keywords*: Lerch prime, Wilson prime

# 1 Notation

The Fermat quotient $q_p(a) = (a^{p-1} - 1)/p$.
The Wilson quotient $W_p = (\{p-1\}! + 1)/p$.
Bernoulli numbers appear in the even index notation of Nörlund ($B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_3 = B_5 = B_7 = \cdots = 0$, etc.).

# 2 The Wilson quotient and the Lerch quotient

In 1899, Glaisher ([5], p. 326) proved that (in the modern notation for the Bernoulli numbers)

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

A new proof of this result appears in Sondow [11], pp. 5–6. The Wilson primes are those that divide their Wilson quotient, the only instances currently known being 5, 13, and 563 ([3], [4]). Clearly, in light of (1), they are characterized by the congruence

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

Now Kummer's congruence for Bernoulli numbers, as extended by Johnson ([7], p. 253) 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 $m = 2$:

$$\frac{B_{2p-2} - 1 + \frac{1}{p}}{2p-2} \equiv \frac{B_{p-1} - 1 + \frac{1}{p}}{p-1} \pmod{p} \quad (p > 2). \tag{3}$$

Multiplying throughout by $p-1$, 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,

$$W_p \equiv B_{2p-2} - B_{p-1} \pmod{p}. \tag{4}$$

This is a result of Lehmer ([9], p. 355), but we think the derivation from Johnson's supplement to Kummer's congruence is illuminating. For a Wilson prime, clearly we have

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

While at first glance this may appear to be a rather pointless reformulation of (2), the significance of this expression will become apparent below.

In 1905, Lerch ([10], p. 472, eq. 4) proved that

$$\sum_{a=1}^{p-1} q_p(a) \equiv W_p \pmod{p} \quad (p > 2). \tag{6}$$

In homage to this important congruence, Jonathan Sondow ([11], p. 3), 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

$$\sum_{a=1}^{p-1} q_p(a) \equiv W_p \pmod{p^2}. \tag{7}$$

The only instances of such primes currently known are $p = 3$, 103, 839, and 2237 [11]; they are Sloane's OEIS sequence no. A197632.

In a 1953 paper by Carlitz ([2], p. 166, eq. 4.2), (1) and (6) are combined and partly strengthened to give

$$\sum_{a=1}^{p-1} q_p(a) \equiv B_{p-1} - 1 + \frac{1}{p} \pmod{p^2} \quad (p > 3). \tag{8}$$

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

$$W_p \equiv B_{p-1} - 1 + \frac{1}{p} \pmod{p^2}, \tag{9}$$

which appears in a slightly different notation in Sondow (p. 5, eq. 6). Incidentally, evaluating the left-hand side of (8) 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

$$\sum_{a=1}^{p-1} q_p(a) = -1 + \frac{1}{p} + \sum_{j=1}^{p} \binom{p}{j} p^{\,j-2} B_{p-j} \quad (p > 3), \tag{10}$$

where $B_{p-j}$ vanishes for all even $j$ except $j = p-1$. This identity, in which the sum is really just the usual expansion of $\frac{1}{p^2}\left\{B_p(p) - B_p\right\}$ with the terms reversed, can be used to obtain congruences like (8) to any desired precision, though (8) is sufficient for our purpose.

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 (6) given by Beeger ([1], p. 83):

$$\begin{aligned} W_p &= \frac{1}{p} \cdot \sum_{a=1}^{p-1} (-1)^a \binom{p-1}{a} \left(a^{p-1} - 1\right) \\ &= \sum_{a=1}^{p-1} (-1)^a \binom{p-1}{a} q_p(a). \end{aligned} \tag{11}$$

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 (11) 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], p. 360), which states:

$$\binom{p-1}{a} \equiv (-1)^a \left\{1 - pH_a + \frac{p^2}{2} H_a^2 - \frac{p^2}{2} H_{a,2}\right\} \pmod{p^3}, \tag{12}$$

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 ([13], p. 285), may be combined with (11) to give the following refinement of Lerch's congruence (6):

$$W_p \equiv \sum_{a=1}^{p-1} q_p(a) - p \cdot \sum_{a=1}^{p-1} H_a\, q_p(a) + \frac{p^2}{2} \cdot \sum_{a=1}^{p-1} H_a^2\, q_p(a) - \frac{p^2}{2} \cdot \sum_{a=1}^{p-1} H_{a,2}\, q_p(a) \pmod{p^3}. \tag{13}$$

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 (12) the weaker

$$\binom{p-1}{a} \equiv (-1)^a \{1 - pH_a\} \pmod{p^2}, \tag{14}$$

and directly from (13) the weaker

$$W_p \equiv \sum_{a=1}^{p-1} q_p(a) - p \cdot \sum_{a=1}^{p-1} H_a\, q_p(a) \pmod{p^2}. \tag{15}$$

The sums over products of Harmonic numbers and Fermat quotients in (13) are relatively intractable, but having recourse to an evaluation of the Wilson quotient by Sun ([12], pp. 210–13) which was obtained by a quite different method, it is known that

$$W_p \equiv \frac{1}{p} - \frac{B_{p-1}}{p-1} + \frac{B_{2p-2}}{2p-2} - \frac{p}{2}\left(\frac{B_{p-1}}{p-1}\right)^2 \pmod{p^2} \quad (p > 3), \tag{16}$$

where the sum of the first two terms in the right-hand side is congruent to $W_p$ (mod $p$), 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 (8) in terms of a Bernoulli number has no such simple counterpart in terms of the Wilson quotient.

## 3 Alternate criteria for Lerch primes

Having reviewed Sondow's original definition of the Lerch primes (7), and an alternate criterion (9) based on Carlitz's congruence, we are now prepared to introduce two additional alternate criteria for Lerch primes, which we refer to as the "third" and "fourth." It will be noted that while the original formulation (7) is a mod $p^2$ condition on the Fermat quotient and the Wilson quotient in combination, these are mod $p$ conditions on the Fermat quotient and Wilson quotient, respectively. The other ingredients in these congruences, Harmonic numbers and Bernoulli numbers, bring a gain in complexity of form which to some extent offsets the simplification of the modulus. However, the existence of mod $p$ tests for Lerch primes has an interesting consequence, which is considered in the next section.

**Theorem 1** (Third criterion for a Lerch prime)**.** *A Lerch prime $p$ is characterized by the congruence*

$$\sum_{a=1}^{p-1} H_a \, q_p(a) \equiv 0 \pmod{p}. \tag{17}$$

*Proof.* Sondow's original definition of a Lerch prime (7) requires that

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

Substituting this into (15) gives

$$p \cdot \sum_{a=1}^{p-1} H_a \, q_p(a) \equiv 0 \pmod{p^2},$$

hence on division throughout by $p$, the result follows. □

**Theorem 2** (Fourth criterion for a Lerch prime)**.** *A Lerch prime $p$ is characterized by the congruence*

$$W_p \equiv \frac{B_{2p-2}}{2p} - \frac{B_{p-1}^2}{2p-2} \pmod{p}. \tag{18}$$

*Proof.* Sun's mod $p^2$ congruence for the Wilson quotient (16) may be combined with the definition of a Lerch prime based on Carlitz's congruence (9) to give yet 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 multiplying throughout by $(p-1)/p$ and cancelling 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. □

## 4 Wilson primes and Lerch primes

Sondow ([11], p. 8) raises the question whether it is possible for a number to be both a Wilson prime and a Lerch prime simultaneously. We address this here.

**Theorem 3** (Condition for a Lerch Prime to be a Wilson prime)**.** *A prime $p$ is simultaneously a Lerch prime and a Wilson prime if it satisfies the congruence*

$$B_{2p-2} \equiv B_{p-1} \pmod{p^2}. \tag{19}$$

*Proof.* Setting the left-hand side of (18) to 0 and multiplying throughout by $2p(p-1)$ gives

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

Substituting the definition of a Wilson prime (2) 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. □

## 5 Conclusion

There is no obvious theoretical reason why a solution to the congruence (19) should not exist, though considering that the search for Wilson primes has already been carried nearly to the limits of existing means of computation, it is doubtful whether an actual example could be discovered. On the other hand, if there is some reason why the congruence is impossible, it would surely be interesting.

The three congruences (3), (5), and (19), may be seen as forming a progression of increasing stringency, with (3) characterizing primes in general, (5) the Wilson primes, and (19) 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 possibly new.

## Acknowledgement

I am grateful to Jonathan Sondow 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] Richard Crandall, Karl Dilcher, & Carl Pomerance, “A search for Wieferich and Wilson primes,” Math. Comp. **66** (1997) 433–449.

[4] Edgar Costa, Robert Gerbicz, & David Harvey, “A search for Wilson primes” (preprint, 2012); available at http://arxiv.org/abs/1209.3436.

[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. Oxford **31** (1899–1900) 321–353.

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

[7] Wells Johnson, “p-adic Proofs of Congruences for the Bernoulli Numbers,” J. Number Theory **7** (1975) 251–265.

[8] Emma Lehmer, “A Note on Wilson’s Quotient,” Amer. Math. Mo. **44** (1937) 237–238.

[9] Emma Lehmer, “On Congruences involving Bernoulli Numbers and the Quotients of Fermat and Wilson,” Ann. of Math., ser. 2, **39** (1938) 350–360.

[10] M. Lerch, “Zur Theorie des Fermatschen Quotienten. . . ,” Math. Ann. **60** (1905) 471–490.

[11] Jonathan Sondow, “Lerch Quotients, Lerch Primes, Fermat-Wilson Quotients, and the Wieferich-non-Wilson Primes 2, 3, 14771” (preprint, 2011); available at http://arxiv.org/abs/1110.3113.

[12] Zhi-Hong Sun, “Congruences concerning Bernoulli numbers and Bernoulli polynomials,” Discrete Appl. Math. **105** (2000) 193–223.

[13] Zhi-Hong Sun, “Congruences involving Bernoulli and Euler numbers,” J. Number Theory **128** (2008) 280–312.