GENERALIZED LERCH PRIMES

René Gy
Bondy, France
rene.gy@numericable.com

Received: 10/25/16, Revised: 8/5/17 Accepted: 2/4/18, Published: 2/19/18

Abstract

We introduce the generalized k-Lerch primes, for any natural number $k \geq 0$. The usual Lerch primes correspond to the case $k = 1$. The Wilson primes together with the primes whose Wilson quotient is 2 mod p lead naturally to the concept of 0-Lerch primes. These generalizations require only elementary modular arithmetic arguments. We show that any prime is a generalized Lerch prime of some sort, except for a restricted list of exceptions. The observed exceptional primes p are shown to satisfy a congruence involving a sum of squares of Fermat quotients, and $2, 11$ and 971 are the only exceptions found so far. Moreover, it is shown that the Wilson-Lerch primes p, if any exist, are the solutions to the supercongruence $(p-1)! + 1 \equiv 0 \bmod p^3$. They also would have to satisfy the congruence involving the sum of squares of Fermat quotients. Finally we raise a couple of open questions.

1. Introduction

The Wilson primes and the Lerch primes are two classes of rare primes which satisfy a congruence modulo p^2 which is only satisfied modulo p by other primes. See, for instance [9] for the definitions, and [9], [3] for recent studies of these kinds of primes, their relationships with Wieferich primes, and their characterization in terms of congruences involving Bernoulli numbers. It is not known whether a prime can simultaneously be a Lerch prime and a Wilson prime [9]. The purpose of the present paper is to show how the notion of a Lerch prime can be generalized. Then, some elementary properties of these generalized Lerch primes will be derived and it will eventually be shown how they can be used to provide new conditions for a Lerch prime to also be a Wilson prime.

2. Notation and Definitions

Let a be a natural number and p a prime integer such that p does not divide a. The *Fermat quotient* $q_p(a)$ and the *Wilson quotient* w_p are the integers defined as

$$q_p(a) := \frac{a^{p-1}-1}{p}, \tag{1}$$

$$w_p := \frac{(p-1)!+1}{p}. \tag{2}$$

When $w_p \equiv 0 \bmod p$, p is said to be a *Wilson prime*. Using Euler's generalization of Fermat's Little Theorem, for all integers $j \geq 1$, the *Euler quotient* is also classically defined as

$$q_{p^j}(a) := \frac{a^{p^{j-1}(p-1)}-1}{p^j}. \tag{3}$$

Theorem 1. *Let $k \geq 0$ be an integer and p an odd prime. Then*

$$\sum_{a=1}^{p-1} q_p(a^k) \equiv k \cdot w_p \pmod{p}.$$

In particular $\sum_{a=1}^{p-1} q_p(a^k) \equiv \sum_{a=1}^{p-1} q_p(a^r) \bmod p$, where r, $0 \leq r \leq p-1$, is the residue class to which k belongs modulo p.

Proof. The proof is well-known [9]. It dates back to the original paper of Lerch [7]. Let a, b be two integers not divisible by p, then

$$\begin{aligned} p \cdot q_p(a \cdot b) &= a^{(p-1)} b^{(p-1)} - 1 \\ &= (p \cdot q_p(a) + 1) \cdot (p \cdot q_p(b) + 1) - 1 \\ &= p^2 q_p(a) q_p(b) + p\left(q_p(a) + q_p(b)\right); \end{aligned}$$

hence, dividing throughout by p and reducing modulo p,

$$q_p(a \cdot b) \equiv q_p(a) + q_p(b) \pmod{p}.$$

Thus

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

so that

$$\frac{(p \cdot w_p - 1)^{p-1} - 1}{p} \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p}.$$

However, modulo p, expanding the numerator on the left-hand side, one only needs to retain terms up to second degree in p and, since p is odd, $(-1)^{p-1} - 1 = 0$ so that the Lerch congruence is obtained:

$$w_p \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p}. \tag{4}$$

Moreover,

$$q_p(a^k) \equiv k \cdot q_p(a) \pmod{p}, \tag{5}$$

and the claim follows. □

Now, for an integer $k \geq 1$, we define the *k-Lerch quotient* of an odd prime p as

$$\ell_{p,k} := \frac{1}{p} \left(\sum_{a=1}^{p-1} q_p(a^k) - k \cdot w_p \right). \tag{6}$$

From Theorem 1, it follows that $\ell_{p,k} \equiv \ell_{p,r} \bmod p$, where r is the residue class to which k belongs modulo p. We will say that an odd prime p is a *k-Lerch prime* when $1 \leq k \leq p-1$ and $\ell_{p,k} \equiv 0 \bmod p$. The case $k = 1$ corresponds to the usual *Lerch quotient* (denoted ℓ_p in the following) and to the usual *Lerch primes*, introduced in [9]. For these,

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

Note that the present generalization of the Lerch quotient is different from that in [9], which pertains to the case where the modulus is composite.

When a prime p is either a Wilson prime or has $w_p \equiv 2 \bmod p$, we shall say that it either belongs to the set $\mathbb{W}$ or to the set $\mathbb{W}_2$ respectively. When a prime p is a k-Lerch prime, $k \geq 1$, we shall say that it belongs to the set $\mathbb{L}_k$.

Remark. The elements of $\mathbb{W}$ and $\mathbb{L}_1$ are the members of the sequences A007540 and A197632 in [8], respectively. For the elements of $\mathbb{W}_2$, see [4] for the range below 50000 and [2] for the range 10^6 to 10^{13}. The gap has been checked by the anonymous reviewer. We can then write:

$$\begin{aligned}
&\mathbb{W} = \{5, 13, 563, \dots\}, \\
&\mathbb{L}_1 = \{3, 103, 839, 2237, \dots\}, \\
&\mathbb{W}_2 = \{19, 1187, 14296621, 16556218163369, \dots\},
\end{aligned}$$

displaying all the currently known elements of $\mathbb{W}$, $\mathbb{L}_1$ and $\mathbb{W}_2$.

3. Some Properties of the Wilson Quotient

From (4), it is evident that Wilson primes are characterized by the congruence

$$\sum_{a=1}^{p-1} q_p(a) \equiv 0 \pmod{p}. \tag{8}$$

In the subsequent developments we shall require the following lemma:

Lemma 1. *Let a, b be two integers not divisible by p and $j \geq 1$ an integer. We have*

$$q_{p^j}(a \cdot b) \equiv q_{p^j}(a) + q_{p^j}(b) \pmod{p^j}.$$

Proof. The proof is very similar to that for Theorem 1, but proceeds from (3):

$$\begin{aligned} p^j \cdot q_{p^j}(a \cdot b) &= a^{p^{j-1}(p-1)} b^{p^{j-1}(p-1)} - 1 \\ &= (p^j \cdot q_{p^j}(a) + 1) \cdot (p^j \cdot q_{p^j}(b) + 1) - 1 \\ &= p^{2j} q_{p^j}(a) q_{p^j}(b) + p^j (q_{p^j}(a) + q_{p^j}(b)), \end{aligned}$$

whence dividing throughout by p^j and reducing modulo p^j, the result follows. □

Theorem 2. *Let $j \geq 0$ be a natural number, p an odd prime. We have*

$$\sum_{a=1}^{p-1} q_p(a^{p^j}) \equiv p^j \cdot w_p \pmod{p^{j+1}}. \tag{9}$$

Moreover,

(i) a necessary and sufficient condition for p to be a Lerch prime is

$$\sum_{a=1}^{p-1} q_p(a) \equiv w_p \pmod{p^2}, \tag{10}$$

(ii) a necessary and sufficient condition for p to belong to $\mathbb{W} \cup \mathbb{W}_2$ is

$$\forall j \geq 1, \quad \sum_{a=1}^{p-1} q_p(a^{p^j}) \equiv p^j \cdot w_p \pmod{p^{j+2}}. \tag{11}$$

Proof. From Theorem 1, we have $\sum_{a=1}^{p-1} q_p(a^{p^j}) \equiv p^j \sum_{a=1}^{p-1} q_p(a) \bmod p$, and since $\sum_{a=1}^{p-1} q_p(a) \equiv w_p \bmod p$, Congruence (9) follows. This result complements the case $j = 0$ covered by Lerch congruence (4). Congruence (10) is merely a restatement of the definition of the Lerch primes. As to the statement (ii) of Theorem 2, from Lemma 1 with $j = 2$, we have

$$\begin{aligned}\sum_{a=1}^{p-1} q_{p^2}(a) &\equiv q_{p^2}\left((p-1)!\right) \pmod{p^2} \\ &\equiv \frac{(p\cdot w_p - 1)^{p(p-1)} - 1}{p^2} \pmod{p^2},\end{aligned}$$

and then

$$p^2 \sum_{a=1}^{p-1} q_{p^2}(a) \equiv \sum_{k=1}^{p(p-1)} p^k w_p^k \binom{p(p-1)}{k} (-1)^k \pmod{p^4}.$$

Now, we have

$$p^k \binom{p(p-1)}{k} = p^{k+1}(p-1) \frac{\prod_{i=1}^{k-1} \left(p(p-1) - i\right)}{k!},$$

so, dividing the last congruence by p^2,

$$\begin{aligned}\sum_{a=1}^{p-1} q_{p^2}(a) &\equiv \sum_{k=1}^{p(p-1)} p^{k-1}(p-1) w_p^k (-1)^k \frac{\prod_{i=1}^{k-1} \left(p(p-1) - i\right)}{k!} \pmod{p^2} \\ &\equiv - \sum_{k=1}^{p(p-1)} p^{k-1}(p-1) w_p^k \frac{\prod_{i=1}^{k-1} (p+i)}{k!} \pmod{p^2} \\ &\equiv -(p-1)w_p - \sum_{k=2}^{p(p-1)} p^{k-2}(p-1) w_p^k \frac{\prod_{i=1}^{k-1} (i\cdot p)}{k!} \pmod{p^2} \\ &\equiv -(p-1)w_p - \sum_{k=2}^{p(p-1)} p^{2k-3}(p-1) \frac{1}{k} w_p^k \pmod{p^2} \\ &\equiv -(p-1)w_p + p\cdot \frac{1}{2} w_p^2 \pmod{p^2}.\end{aligned}$$

But from (3) we have

$$p\cdot q_{p^2}(a) = \frac{a^{p(p-1)} - 1}{p} = q_p(a^p).$$

Substituting this into the last congruence above and multiplying throughout by p gives

$$\sum_{a=1}^{p-1} q_p(a^p) \equiv p\cdot w_p - p^2 w_p \left(1 - \frac{1}{2} w_p\right) \pmod{p^3},$$

which proves the statement (ii) of Theorem 2 in the case $j = 1$. Now,

$$\sum_{a=1}^{p-1} q_p(a^{p^{j+1}}) - \sum_{a=1}^{p-1} p \cdot q_p(a^{p^j}) = \sum_{a=1}^{p-1} \frac{a^{p^{j+1}(p-1)} - 1}{p} - \sum_{a=1}^{p-1} \left(a^{p^j(p-1)} - 1\right)$$

$$= \sum_{a=1}^{p-1} \frac{(p \cdot q_p(a) + 1)^{p^{j+1}} - 1}{p} - \sum_{a=1}^{p-1} \left((p \cdot q_p(a) + 1)^{p^j} - 1\right).$$

Expanding the binomial expressions in the right-hand side and retaining only the terms of order less than p^{j+3}, we have

$$\sum_{a=1}^{p-1} q_p(a^{p^{j+1}}) - \sum_{a=1}^{p-1} p \cdot q_p(a^{p^j}) \equiv \frac{1}{2} p^{j+2} \left(p^{j+1} - p^j\right) \sum_{a=1}^{p-1} q_p^2(a) \pmod{p^{j+3}}.$$

Then, the right-hand side, which is divisible by $p^{2j+2} \geq p^{j+3}$ for $j \geq 1$, vanishes, leaving

$$\sum_{a=1}^{p-1} q_p(a^{p^{j+1}}) \equiv p \sum_{a=1}^{p-1} q_p(a^{p^j}) \pmod{p^{j+3}},$$

which establishes the statement (ii) of Theorem 2 in the general case $j \geq 1$, by induction, since it has already been proven for $j = 1$. $\square$

4. Properties of the Lerch Quotient

Lemma 2. *Let k and a be natural numbers and p a prime that does not divide a. Then*

$$q_p(a^k) \equiv k \cdot q_p(a) + p \cdot q_p^2(a) \frac{k(k-1)}{2} \pmod{p^2}. \tag{12}$$

Proof. We have $q_p(a^k) = \frac{1}{p}(a^{k(p-1)} - 1) = \frac{1}{p}\left((p \cdot q_p(a) + 1)^k - 1\right)$, then discarding the terms divisible by p^2 in the right-hand side, the claim follows. $\square$

Theorem 3. *Let p be an odd prime, ℓ_p the usual Lerch quotient and k a natural number, $1 \leq k \leq p-1$. A necessary and sufficient condition for p to be a k-Lerch prime is:*

$$\ell_p + \frac{k-1}{2} \sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \pmod{p}. \tag{13}$$

Proof. Substituting the evaluation of $q_p(a^k)$ from Lemma 2 into Equation (6), we have

$$p \cdot \ell_{p,k} \equiv \sum_{a=1}^{p-1} \left(k \cdot q_p(a) + p \cdot q_p^2(a) \frac{k(k-1)}{2} \right) - k \cdot w_p \pmod{p^2}.$$

Recall that, by definition, p is a k-Lerch prime if and only if $p|\ell_{p,k}$. Then, an equivalent statement is:

$$k \left(\sum_{a=1}^{p-1} q_p(a) - w_p \right) + p \cdot \frac{k(k-1)}{2} \sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \pmod{p^2},$$

so that

$$k \cdot p \cdot \ell_p + p \cdot \frac{k(k-1)}{2} \sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \pmod{p^2}$$

and the result follows, since p does not divide k. □

Although the original formulation of the k-Lerch quotient (6) would be degenerate in the case $k = 0$, it is nonetheless possible to obtain a result analogous to (13) in the case $k = 0$. This will be shown in the following theorem, which is another characterization of the primes in $\mathbb{W} \cup \mathbb{W}_2$.

Theorem 4. *Let p be an odd prime, ℓ_p the usual Lerch quotient. We have*

$$\ell_p - \frac{1}{2} \sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \pmod{p}. \tag{14}$$

if and only if $p \in \mathbb{W} \cup \mathbb{W}_2$.

Proof. Taking $j = 1$ in (11), we have

$$p \cdot w_p \equiv \sum_{a=1}^{p-1} q_p(a^p) \pmod{p^3}.$$

Developing the right-hand side by the same method as in the proof of Lemma 2, we have

$$p \cdot w_p \equiv \sum_{a=1}^{p-1} \left(p \cdot q_p(a) + p \cdot q_p^2(a) \frac{p(p-1)}{2} \right) \pmod{p^3},$$

and therefore, dividing throughout by p,

$$w_p \equiv \sum_{a=1}^{p-1} q_p(a) - \frac{1}{2}p\sum_{a=1}^{p-1} q_p^2(a) \pmod{p^2}. \tag{15}$$

The required results follows by rearranging and again dividing throughout by p:

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

$\square$

Remark. We can then define the set of the 0-*Lerch primes* as $\mathbb{L}_0 := \mathbb{W} \cup \mathbb{W}_2$, by analogy with (13).

5. On the Existence of Wilson-Lerch Primes

We are now prepared to state a new necessary condition for a prime to be simultaneously a Lerch prime and a Wilson prime:

Theorem 5. *A necessary condition for p to be simultaneously a Lerch prime and a Wilson prime is*

$$\sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \pmod{p}. \tag{16}$$

Proof. From (13), with $k = 1$, for a Lerch prime $\ell_p \equiv 0 \pmod{p}$, while from (14), for a Wilson prime $\ell_p - \frac{1}{2}\sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \pmod{p}$. The result follows immediately. $\square$

Let $\mathbb{S}$ be the set of primes p characterized by (16). The smallest elements of $\mathbb{S}$ are 2, 11, and 971. They are easily obtained by a brute-force search with a laptop computer. Direct computation of the sum in (16) rapidly becomes impractical for larger values of p, but a congruence given by Emma Lehmer ([6], p. 353, eq. 15) enables us to show that, when p is odd:

$$\sum_{a=1}^{p-1} q_p^2(a) \equiv \frac{1}{p}\left(B_{2p-2} - 2B_{p-1} + 1 - \frac{1}{p}\right) \pmod{p}. \tag{17}$$

Then, the odd primes p in $\mathbb{S}$ are characterized by

$$B_{p-1} - 1 + \frac{1}{p} \equiv \frac{B_{2p-2} - 1 + \frac{1}{p}}{2} \pmod{p^2}, \tag{18}$$

where B_j is a Bernoulli number, in the even index notation. Although Bernoulli numbers are more computationally complex than the Fermat quotients in (16), in most dedicated number-theory applications such as PARI/GP their evaluation in modular arithmetic is sufficiently optimized to result in better runtimes. Congruence (18) has been checked by the anonymous reviewer up to 427000 without finding any new element in $\mathbb{S}$.

Theorem 6. *All odd primes p, with the possible exceptions of those belonging to $\mathbb{S}$, satisfy*

$$\ell_p + \frac{k-1}{2}\sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \pmod{p} \tag{19}$$

for some value of k, $0 \le k \le p-1$, in at least one way. Furthermore, every prime not belonging to $\mathbb{S}$ satisfies (19) in precisely one way.

Proof. This congruence represents the union of (13) and (14), each of which covers only a more restricted range of k. Here, k runs through a complete residue system modulo p, and therefore, unless p belongs to $\mathbb{S}$, so must $\frac{k-1}{2}\sum_{a=1}^{p-1} q_p^2(a)$, and one of these p distinct values is the complement of ℓ_p modulo p. Thus, any odd prime not in $\mathbb{S}$ is represented by (19). Furthermore, unless p belongs to $\mathbb{S}$ this representation is guaranteed to be unique. For suppose that p were simultaneously an r_1-Lerch prime and an r_2-Lerch prime with $0 \le r_1 < r_2 \le p-1$; then by equation (13) we should have $(r_1 - r_2)\frac{1}{2}\sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \bmod p$, but since by hypothesis p does not divide the sum in the left-hand side, it must divide $r_1 - r_2$. Hence $r_1 \equiv r_2 \bmod p$, which is a contradiction. ☐

Corollary 1. *Odd primes p in $\mathbb{S}$ satisfy*

$$\ell_p + \frac{k-1}{2}\sum_{a=1}^{p-1} q_p^2(a) \equiv 0 \pmod{p} \tag{20}$$

with $0 \le k \le p-1$, either for every value of k or for no value of k.

Proof. For odd primes $p \in \mathbb{S}$, (20) simply asserts that $\ell_p \equiv 0 \pmod{p}$ irrespective of the value of k, and this congruence is either true or it is not. ☐

Remark. Neither 11 nor 971, the known odd elements of $\mathbb{S}$, satisfies (20) for any value of k.

Theorem 7. *The following is a necessary and sufficient criterion for a prime p to be simultaneously a Lerch prime and a Wilson prime:*

$$w_p \equiv 0 \pmod{p^2}. \tag{21}$$

Note that this is a supercongruence, not the congruence (8) that characterizes the usual Wilson primes. In other words, the Wilson-Lerch primes are the super-Wilson primes, should any exist.

Proof. The statement of this theorem, and its proof, are due to the anonymous reviewer. Recall from (15) this necessary and sufficient condition for p to belong to $\mathbb{W} \cup \mathbb{W}_2$:

$$w_p \equiv \sum_{a=1}^{p-1} q_p(a) - \frac{1}{2} p \sum_{a=1}^{p-1} q_p^2(a) \pmod{p^2}. \tag{22}$$

A congruence of Carlitz [1] states that for $p > 3$,

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

Substituting Carlitz's result into Lehmer's congruence (17) multiplied throughout by p, gives

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

Substituting this result in turn into (22) gives

$$w_p \equiv \frac{3}{2} \sum_{a=1}^{p-1} q_p(a) - \frac{1}{2} \left(B_{2p-2} - B_{p-1} \right) \pmod{p^2}.$$

Now Dobson ([3], p. 6, Theorem 1) showed that $B_{2p-2} \equiv B_{p-1} \bmod p^2$ is a necessary and sufficient condition for p to be simultaneously a Lerch prime and a Wilson prime. Under this condition the second term on the right hand side vanishes, leaving

$$w_p \equiv \frac{3}{2} \sum_{a=1}^{p-1} q_p(a) \pmod{p^2}.$$

But, if we compare this congruence with the original criterion for p to be a Lerch prime (7), we see that together they imply

$$\frac{3}{2} \sum_{a=1}^{p-1} q_p(a) \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p^2},$$

which is a contradiction unless $\sum_{a=1}^{p-1} q_p(a) \equiv 0 \bmod p^2$, leading to (21). Of course the congruence just mentioned also implies $\sum_{a=1}^{p-1} q_p(a) \equiv 0 \bmod p$, guaranteeing that p is a Wilson prime (8) and thereby establishing the sufficiency of (21) even though we began in (22) with a condition that pertains to any prime in $\mathbb{W} \cup \mathbb{W}_2$. $\square$

6. Open Questions

In the following table, some small primes p, $p < 15000$, are sorted according to whether they belong to $\mathbb{S}$ or to $\mathbb{L}_k$ (the k-Lerch primes) for small k, $0 \le k \le 36$.

	$\mathbb{L}_0$		$\mathbb{L}_k$																	
$\mathbb{S}$	$\mathbb{W}_2$	$\mathbb{W}$	k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2	19	5		3	.	7	17	73	.	317	53	191	71	23	.	.	.	.	3011	41
11	1187	13		103	.	233	.	.	.	.	.	.	.	29	.	.	.	.	.	.
971	.	563		839	.	.	.	.	.	.	.	.	.	1499	.	.	.	.	.	.
.	.	.		2237	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.		.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

$\mathbb{L}_k$ (continued)																		
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
6343	.	239	67	137	.	281	37	577	1481	31	.	43	.	.	47	.	107	3511
.	.	1693	2011	.	.	1069	.	.	1483	.	.	.	.	.	.	.	1453	.
.	.	.	.	.	.	.	.	.	4273	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	10223	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Table 1: The k-Lerch primes smaller than 15000, for $k \le 36$, together with the known primes in $\mathbb{S}$.

Conjecture 1. $\{\mathbb{S}, \mathbb{L}_k; k \ge 0\}$ is a partition of $\mathbb{P}$, the set of all prime numbers.

If Conjecture 1 is wrong, there would be an element p of $\mathbb{S}$ that would simultaneously belong to the $\mathbb{L}_k$ for all $1 \le k \le p-1$, to either $\mathbb{W}$ or $\mathbb{W}_2$ and, of course, to $\mathbb{S}$. This would be a rather extraordinary prime number, for all the many stringent conditions it would satisfy. If true, this would imply that no Wilson prime can simultaneously be a Lerch prime and that there are no super-Wilson primes.

Do k-Lerch primes exist for every positive integer k? The question is raised because for some k, like $k = 2$, there is no small k-Lerch prime in Table 1. But, thanks to the following derivations due to the anonymous reviewer and presented in a final section hereafter, the search for 2-Lerch prime can be pushed further and eventually, it is found that 207953 is a 2-Lerch prime. We then venture the following conjecture.

Conjecture 2. k-Lerch primes exist for every $k \ge 0$.

7. Alternate Formulations for the k-Lerch Primes and for the Primes in $\mathbb{S}$

In this section, we express the original criterion (6) for the k-Lerch primes in a more computationally tractable form, pointed out by the anonymous reviewer. To this end, we recall Kummer's famous congruence for the Bernoulli numbers, which states that, for $b \not\equiv 0 \bmod p-1$:

$$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \frac{B_b}{b} \pmod{p}.$$

In 1975, Johnson [5] extended this result to the case $b=0$ ($k \neq 0$), showing that

$$\frac{B_{k(p-1)} - 1 + \frac{1}{p}}{k(p-1)} \equiv \frac{B_{p-1} - 1 + \frac{1}{p}}{p-1} \pmod{p}, \tag{23}$$

where the common terms $p-1$ in the denominators are retained in analogy with Kummer's congruence. In 1997, Z.H. Sun [10] published a generalization of this extension to the modulus p^2, here rearranged to bring out the resemblance to Johnson's result:

$$\frac{B_{k(p-1)} - 1 + \frac{1}{p}}{k(p-1)} \equiv (k-1)\frac{B_{2(p-1)} - 1 + \frac{1}{p}}{2(p-1)} - (k-2)\frac{B_{p-1} - 1 + \frac{1}{p}}{p-1} \pmod{p^2}. \tag{24}$$

Next, we note Glaisher's congruence for the Wilson quotient (see [9]), which states that for all primes $p > 3$,

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

Comparing this congruence with (23), we see that

$$w_p \equiv \frac{1}{k}\left(B_{k(p-1)} - 1 + \frac{1}{p}\right) \pmod{p}$$

also holds for every positive value of k and $p \geq 5$. We are now prepared to state our last theorem:

Theorem 8. *Let $p > 3$ be a prime and k an integer such that $1 \leq k \leq p-1$. A necessary and sufficient condition for p to be a k-Lerch prime is*

$$w_p \equiv \frac{1}{k}\left(B_{k(p-1)} - 1 + \frac{1}{p}\right) \pmod{p^2}. \tag{25}$$

Proof. In the proof of Theorem 3, we have seen that a k-Lerch prime is characterized by the congruence

$$w_p \equiv \sum_{a=1}^{p-1} q_p(a) + \frac{k-1}{2} p \sum_{a=1}^{p-1} q_p^2(a) \pmod{p^2}.$$

Evaluating the sums in the right-hand side using the congruences of Carlitz and Lehmer mentioned in the proof of Theorem 7, we obtain

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

that is

$$w_p \equiv (k-1)\frac{B_{2(p-1)} - 1 + \frac{1}{p}}{2} - (k-2)\left(B_{p-1} - 1 + \frac{1}{p}\right) \pmod{p^2}. \tag{26}$$

Then, applying Sun's congruence (24) into (26) yields (25). □

Remark. As noted above, this congruence is satisfied modulo p by all primes $p > 3$ and $k > 0$. For the case $k = 1$, it is implied in [9], and stated but with the condition $p > 3$ missing in [3].

Remark. Theorem 8 was used by the reviewer to look for 2-Lerch primes up to 386000 and $p = 207953$ was found. However (26) is more efficient than (25) to look for k-Lerch primes, because the expressions involving Bernoulli numbers can be repurposed. The reviewer then made use of (26) to expand Table 1 up to $p < 381000$. Newly found k-Lerch primes are given in the following table. Some of them would fill in empty columns of Table 1 and this provides further heuristic support for Conjecture 2.

$k=2$	$k=3$	$k=7$	$k=14$	$k=18$	$k=19$	$k=23$	$k=31$	$k=34$
207953	49043	58943	15791	159899	20903	27653	166013	68711
					61933			242257

Table 2: The k-Lerch primes in the range 15000 to 381000, for $k \leq 36$.

Finally, we also give another formulation for the odd primes in $\mathbb{S}$. Recall from (18) that the odd primes in $\mathbb{S}$ can be characterized by

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

Substituting this condition into Sun's congruence (24) gives, for all $k \neq 0$:

$$\frac{B_{k(p-1)} - 1 + \frac{1}{p}}{k(p-1)} \equiv \frac{B_{p-1} - 1 + \frac{1}{p}}{p-1} \pmod{p^2}, \tag{27}$$

which is a supercongruence version of Johnson's congruence (23). It does not seem to have been previously considered whether (23) could be satisfied modulo p^2, and then, by analogy with Wilson, Lerch and other similar congruences, the odd elements in $\mathbb{S}$ might be named Johnson primes.

Acknowledgements. I am indebted to the anonymous referee, not only for many stylistic and organization improvements of the manuscript, but also for the substantial additions of Theorem 7 and Section 7, and for extended numerical computations.

References

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

[2] E. Costa, R. Gerbicz, and D. Harvey. A search for Wilson primes, *Math. Comp.* **83** (2014), 2071-3091.

[3] J. Dobson. A characterization of Wilson-Lerch primes, *Integers* **16** (2016), #A51.

[4] C. Fröberg. Investigation of the Wilson remainders in the interval $3 < p < 50,000$, *Ark. Mat.* **4** (1961), 479-499.

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

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

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

[8] N. J. A. Sloane. The On-Line Encyclopedia of Integer Sequences, published electronically at `https://oeis.org`.

[9] 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.

[10] Z.-H. Sun. Congruences for Bernoulli numbers and Bernoulli polynomials. *Discrete Math.* **163** (1997), 153-163.