1 INTRODUCTION

The *Fermat quotient of* $p$ *base* $a$, if prime $p \nmid a$, is the integer

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

and the *Wilson quotient of* $p$ *is the integer*

$$w_p := \frac{(p-1)! + 1}{p}.$$
A prime $p$ is a Wilson prime if $p \mid w_p$, that is, if the supercongruence
\[(p - 1)! + 1 \equiv 0 \pmod{p^2}\]
holds. (A supercongruence is a congruence whose modulus is a prime power.)
For $p = 2, 3, 5, 7, 11, 13$, we find that
\[w_p \equiv 1, 1, 0, 5, 1, 0 \pmod{p}\]
and so the first two Wilson primes are 5 and 13. The third and largest known one is 563, uncovered by Goldberg in 1953.

Vandiver in 1955 famously said:

*It is not known if there are infinitely many Wilson primes. This question seems to be of such a character that if I should come to life any time after my death and some mathematician were to tell me that it had definitely been settled, I think I would immediately drop dead again.*
2 LERCH QUOTIENTS AND LERCH PRIMES

In 1905 Lerch proved a congruence relating the Fermat and Wilson quotients of an odd prime.

Lerch’s Formula. If a prime $p$ is odd, then

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

that is,

$$\sum_{a=1}^{p-1} a^{p-1} - p - (p - 1)! \equiv 0 \pmod{p^2}.$$
2.1 Lerch Quotients

Lerch’s formula allows us to introduce the Lerch quotient of an odd prime, by analogy with the classical Fermat and Wilson quotients of any prime.

**Definition 1.** The *Lerch quotient* of an odd prime $p$ is the integer

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

For instance, the Lerch quotient of $p = 5$ is

$$
\ell_5 = \frac{0 + 3 + 16 + 51 - 5}{5} = \frac{1 + 16 + 81 + 256 - 5 - 24}{25} = 13.
$$
Among the Lerch quotients $\ell_p$ of the first 1000 odd primes, only $\ell_5 = 13$ is itself a prime number. On the other hand, the Wilson quotients $w_5 = 5$, $w_7 = 103$, $w_{11} = 3298891$, and $w_{29} = 10513391193507374500051862069$, as well as $w_{773}$, $w_{1321}$, and $w_{2621}$, are themselves prime.

2.2 Lerch Primes

We define Lerch primes by analogy with Wilson primes.

**Definition 2.** An odd prime $p$ is a *Lerch prime* if $p \mid \ell_p$, that is, if

$$\sum_{a=1}^{p-1} a^{p-1} - p - (p-1)! \equiv 0 \pmod{p^3}.$$
For \( p = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, \ldots \),
we find that
\[
\ell_p \equiv 0, 3, 5, 5, 6, 12, 13, 3, 7, 19, 2, 21, 34, 33, 52, 31, 51, 38, 32, 25, 25, 25, 53, 22, 98, 0, \ldots \pmod{p},
\]
and so the first two Lerch primes are 3 and 103.

We found the Lerch primes 3, 103, 839, 2237 and no others up to \( p \leq 1000003 \).

Marek Wolf, using *Mathematica*, has computed that there are no Lerch primes in the intervals:
\[
1000003 \leq p \leq 4496113, \\
18816869 \leq p \leq 18977773, \\
32452867 \leq p \leq 32602373.
\]
2.3 Generalizations

Euler and Gauss extended Fermat’s little theorem and Wilson’s theorem to congruences with a composite modulus \( n \), respectively. The corresponding generalizations of Fermat and Wilson quotients and Wilson primes are called Euler quotients \( q_n(a) \), generalized Wilson quotients \( w_n \), and Wilson numbers \( n \mid w_n \).

In 1998 Agoh et al extended Lerch’s formula to a congruence between the \( q_n(a) \) and \( w_n \). So one can define and study generalized Lerch quotients \( \ell_n \) and Lerch numbers \( n \mid \ell_n \).

2.4 Open Problems I

1. Is \( \ell_5 = 13 \) the only prime Lerch quotient?
2. Is there a fifth Lerch prime? Are there infinitely many?
Of the 78498 primes $p < 10^6$, only four are Lerch primes. Thus the answer to the next question is clearly yes; the only thing lacking is a proof!

3. Do infinitely many non-Lerch primes exist?

As the known Lerch primes 3, 103, 839, 2237 are distinct from the known Wilson primes 5, 13, 563, we may ask:

4. Is it possible for a number to be a Lerch prime and a Wilson prime simultaneously?

Denoting the $n$th prime by $p_n$, the known Wilson primes are $p_3, p_6, p_{103}$. The primes among the indices 3, 6, 103, namely, 3 and 103, are Lerch primes. This leads to the question:

5. If $p_n$ is a Wilson prime and $n$ is prime, must $n$ be a Lerch prime?
3 FERMAT-WILSON QUOTIENTS AND THE WIEFERICH-NON-WILSON PRIMES 2, 3, 14771

Suppose that a prime \( p \) is not a Wilson prime, so \( p \nmid w_p \). Then in the Fermat quotient \( q_p(a) \) of \( p \) base \( a \), we may take \( a = w_p \).

**Definition 3.** If \( p \) is a non-Wilson prime, then the *Fermat-Wilson quotient of \( p \)* is the integer

\[
q_p(w_p) = \frac{w_p^{p-1} - 1}{p}.
\]

For short we write

\[
g_p := q_p(w_p).
\]

The first five non-Wilson primes are 2, 3, 7, 11, 17. As \( w_2 = w_3 = 1 \) \( w_7 = 103 \), and \( w_{11} = 329891 \), the first four Fermat-Wilson quotients are

\[
g_2 = g_3 = 0,
\]

\[
g_7 = \frac{103^6 - 1}{7} = 170578899504,
\]
and

\[ g_{11} = \frac{329891^{10} - 1}{11} \]
\[ = 1387752405580695978098914368989316131852701063520729400. \]

The fifth one, \( g_{17} \), is a 193-digit number.

3.1 The GCD of all Fermat-Wilson quotients

We saw that at least one Lerch quotient \( \ell_5 \) and seven Wilson quotients \( w_5, w_7, w_{11}, w_{29}, w_{773}, w_{1321}, w_{2621} \) are prime numbers. What about Fermat-Wilson quotients?

**Theorem 1.** The greatest common divisor of all Fermat-Wilson quotients is 24. In particular, \( q_p(w_p) \) is never prime.
3.2 Wieferich primes base $a$

Given an integer $a$, a prime $p$ is called a *Wieferich prime base $a$* if the supercongruence

$$a^{p-1} \equiv 1 \pmod{p^2}$$

holds. For instance, 11 is a Wieferich prime base 3, because

$$3^{10} - 1 = 59048 = 11^2 \cdot 488.$$ 

3.3 The Wieferich-non-Wilson primes
2, 3, 14771

Let us consider Wieferich primes $p$ base $a$, where $a$ is the Wilson quotient of $p$.

**Definition 4.** Let $p$ be a non-Wilson prime, so that its Fermat-Wilson quotient $q_p(w_p)$ is an integer. If $p \mid q_p(w_p)$, that is, if the supercongruence

$$w_p^{p-1} \equiv 1 \pmod{p^2}$$

(1)
holds, then \( p \) is a Wieferich prime base \( w_p \), by definition. In that case, we call \( p \) a \textit{Wieferich-non-Wilson prime}, or \textit{WW prime} for short.

For the non-Wilson primes \( p = 2, 3, 7, 11, 17, 19, 23, \ldots \), the Fermat-Wilson quotients \( q_p(w_p) = g_p \) are congruent modulo \( p \) to
\[
g_p \equiv 0, 0, 6, 7, 9, 7, 1, \ldots \pmod{p}.
\]
In particular, 2 and 3 are WW primes. But they are trivially so, because \( g_2 \) and \( g_3 \) are equal to zero.

Is there a “non-trivial” WW prime? Perhaps surprisingly, the answer is yes and the smallest one is 14771. It is “non-trivial” because \( g_{14771} \neq 0 \). In fact,
\[
g_{14771} = \left(\frac{14770! + 1}{14771}\right)^{14770} - 1 > 10^{8 \times 10^8},
\]
so that the number \( g_{14771} \) has more than 800 million decimal digits.
Michael Mossinghoff has computed that the only WW primes $< 10^7$ are $2, 3, 14771$.

3.4 Open Problems II

We conclude with three more open problems.

6. Can one prove that $14771$ is a WW prime (i.e., that $14771$ divides $g_{14771}$) without using a computer?

Such a proof would be analogous to those given by Landau and Beeger that $1093$ and $3511$, respectively, are Wieferich primes base $2$.

7. Is there a fourth WW prime? Are there infinitely many?

8. Do infinitely many non-WW primes exist?
A preprint is at:

THANKS FOR YOUR ATTENTION!