A note on the Voronoi congruences and the residue of the Fermat quotient

Claire Levaillant

August 31, 2021

Abstract

We prove a congruence on the residue of the Fermat quotient in base \( a \) which arises from a generalization of the Voronoi congruences and from some other congruences on sums and weighted sums of divided Bernoulli numbers. As an application in the base 2 case, we retrieve a congruence for the generalized harmonic number \( H_{2, \frac{p-1}{2}} \), a generalization originally due to Sun of a classical congruence known since long for the harmonic number \( H_{\frac{p-1}{2}} \) as a special case of the Lerch formula. We find a sharpening of the Voronoi congruences that is different from the one of Johnson and more computationally efficient. We prove an additional related congruence, which specialized to base 2, allows to retrieve several congruences that were originally due to Lehmer.

1 Past interest in computing the residue of the Fermat quotient in base \( a \)

Computing the residue of the Fermat quotient \( q_a \) in general base \( a \) has become important to mathematicians since the beginning of the twentieth century ever since young Arthur Wieferich showed in 1909 that if the first case of Fermat’s last theorem (FLT) is false for a prime \( p \geq 5 \) then this prime is such that \( q_2 = 0 \mod p \) [26]. Such a prime got later called a Wieferich prime in his honor.

**FLT.** For \( n \geq 3 \), the equation \( X^n + Y^n = Z^n \) has no solutions in integers \( X,Y,Z \) with \( XYZ \neq 0 \).

Since it was proven by Fermat for \( n = 4 \) and by Euler for \( n = 3 \), it then sufficed to prove it when \( n \) is a prime \( p \geq 5 \).

**First case of FLT.** For fixed prime \( p \geq 5 \), there is no integer solution to \( X^p + Y^p = Z^p \) with \( XYZ \) prime to \( p \).
The first Wieferich prime 1093 was found by Meissner in 1913 [16] and the second 3511 was found by Beeger in 1922 [2]. As of today, there are no other known Wieferich primes. Wells Johnson noticed in 1977 [10] that the two numbers that are one less than the two known Wieferich primes have repetitions in their representations in base 2 and other bases, such as

\[ 1092 = 10001000100 \text{ in base 2} \quad 3510 = 110110110110 \text{ in base 2} \]

\[ 1092 = 444 \text{ in base 16} \quad 3510 = 6666 \text{ in base 8} \]

Wieferich’s result from 1909 got extended to the other primes \( q \) in 1910 by Mirimanoff [18] (two known base 3 Wieferich primes, namely 11 and 1006003 found by Kloss in 1965), \( q_5 \) in 1914 by Vandiver [21] (six known base 5 Wieferich primes), \( q_p \) with \( p \leq 31 \) prime in 1917 by Pollaczek, \( q_p \) with \( p \leq 89 \) prime in 1988 by Granville and Monagan [8] and finally \( q_p \) with \( p \leq 113 \) prime in 1994 by Suzuki [20], at which point FLT was proven and interest dropped.

## 2 Main theorem on the residue of the Fermat quotient in base \( a \)

Let \( p \) be an odd prime and let \( a \) be an integer with \( 1 \leq a \leq p-1 \). The main purpose of this note is to use the results of [13] and [15] providing the respective residues of a sum of the first \( (p-2) \) divided Bernoulli numbers and of a powers of \( a \) weighted sum of the first \( (p-2) \) divided Bernoulli numbers in order to find a nice expression for the residue of the Fermat quotient \( q_a \) in base \( a \). We recall these results below. In what follows, \( w_p \) denotes the Wilson quotient.

**Result 1.** Issued from Congruence (9) in Theorem 6 of [13]

\[
\sum_{i=1}^{p-2} B_i = w_p \mod p
\]

**Result 2.** Issued from Proposition 2 of [13].

Let \( a \) be any integer with \( 1 \leq a \leq p-1 \). Then, we have:

\[
\sum_{i=1}^{p-2} \frac{B_i}{a^i} = q_a + w_p \mod p
\]

The proof of the first fact is based on the combinatorial interpretation of the unsigned Stirling number of the first kind \( \left[ \begin{array}{c} p \\ s \end{array} \right] \). Such a number namely counts the number of permutations of the symmetric group \( \text{Sym}(p) \) which decompose into a product of \( s \) disjoint cycles. By summing these numbers over the cycles we get the order of the symmetric group \( \text{Sym}(p) \), that is \( p! \). In 1900, Glaisher provided the expansion of these numbers to the modulus \( p^2 \) [5]. By using Glaisher’s formulas, we easily derive Result 1.
The proof of the latter fact is based on the more common definition of the unsigned Stirling numbers of the first kind, expanding the falling factorial and specializing $x = -a$ in both factored and expanded form. The result then follows again from the Glaisher formulas.

The current paper arose from an attempt to find a similar congruence when the divided Bernoulli numbers are replaced with the ordinary ones. A natural idea consisted in remembering that the residue of $B_i$ is the first potentially nonzero residue in the $p$-adic expansion of a sum of $i$-th powers of the first $(p - 1)$ integers. The most general congruence for the sums of powers of integers gets provided by Zhi-Hong Sun in [19]. In [14], using Sun’s method, we pushed his expansion to the modulus $p^4$:

$$S_t = \sum_{a=1}^{p-1} a^t = pB_t + \frac{p^2}{2} tB_{t-1} + \frac{p^3}{6} t(t-1)B_{t-2} + \frac{p^4}{24} t(t-1)(t-2)B_{t-3} \mod p^4$$

(1)

This is also a good time to recall the fundamental consequence of the Von Staudt-Clausen’s theorem: the denominator of a Bernoulli number $B_i$ consists of products of primes $p$ with multiplicities one, such that $p - 1$ divides $i$ [24][3].

In what follows, $i$ is a positive integer prime to $p$ and incongruent to 1 modulo $(p - 1)$.

For a $p$-adic integer $x \in \mathbb{Z}_p$, we denote by $(x)_i$ its $(i + 1)$-th residue in its $p$-adic Hensel expansion. See for instance [7]. We have under the given assumptions on $i$ and using the notations from before:

$$S_i = p B_i \mod p^2$$

(2)

Then,

$$pB_i a^i = \sum_{b=1}^{p-1} \left( \frac{b}{a} \right)^i = \sum_{b=1}^{p-1} \left( \frac{b}{a} \right)_0 + p \sum_{b=1}^{p-1} \left( \frac{b}{a} \right)_1 \left( \frac{b}{a} \right)_0^{i-1} \mod p^2$$

(3)

In the middle sum of (3), the product $ba^{-1}$ with $a^{-1}$ the inverse of $a$ modulo $p$ must be treated modulo $p^2$, while in the first sum of the right hand side this product is now treated modulo $p$. Then, for fixed $a$, the product $ba^{-1}$ takes all the values between 1 and $p - 1$ exactly once when $b$ varies between 1 and $p - 1$. Whence, that sum is nothing else than a sum of $i$-th powers of the first $p - 1$ integers which is congruent to $pB_i \mod p^2$. Moreover, the second coefficient in the $p$-adic expansion of $ba^{-1}$ can be written in terms of integer part as

$$\left( \frac{b}{a} \right)_1 = \left[ \frac{ba^{-1}}{p} \right],$$

(4)

where the inverse of $a$ is taken modulo $p$. Simplifying the congruence by $p$ and dividing by $i$ leads to

$$\frac{B_i}{a^i} - B_i = \sum_{b=1}^{p-1} \left[ \frac{ba^{-1}}{p} \right] (ba^{-1})_{0}^{i-1} \mod p$$

(5)
In the case when \( i \) is even and with some slightly different assumption on \( i \), namely that \( i \) is incongruent to 0 modulo \((p - 1)\), we obtain the fundamental Voronoi congruence where the integer \( a \) has been replaced with its inverse. This famous congruence got generalized to the modulus \( p^2 \) by Johnson in [9] still for the even \( i \)'s and under the assumption that \( i \) is incongruent to 2 modulo \((p - 1)\) and \( a \neq 1 \). Formerly in [23], Vandiver had built upon the Voronoi congruence s by showing under the same assumption as Voronoi’s that

\[
(1 - a^i)B_i = \sum_{n=1}^{a} \left[ \frac{np}{a} \right] \sum_{b=1}^{(ab)^{i-1}} \mod p
\]

This is the congruence that was extensively used by many authors to compile tables for the irregular primes. Kümmer had shown that FLT holds true when the exponent is a regular prime [11].

We now operate on Congruence (5) by summing over the \( i \)'s for the range \( 2 \leq i \leq p - 3 \). The left hand side gets processed through Results 1 and 2. The right hand side gets processed through the summation of a geometric series when \( b \) is distinct from \( a \) and directly for \( b = a \). In the first case, it yields:

\[-1 - (ba^{-1})^{-1} - (ba^{-1})^{-2} \mod p\]

In the second case, it yields \( p - 4 \) that is \(-4 \mod p\). Hence the following statement.

**Theorem 1.** Let \( a \) be an integer with \( 1 \leq a \leq p - 1 \). The residue of the Fermat quotient in base \( a \) can be computed as follows.

\[
q_a = \frac{1}{2}(1 - a^{-1}) - \sum_{b=1}^{p-1} \left[ \frac{b(a^{-1})_a}{p} \right] - a \sum_{b=1}^{p-1} \left[ \frac{b(a^{-1})_a}{p} \right] \frac{1}{b}
\]

\[-a^2 \sum_{b=1}^{p-1} \left[ \frac{b(a^{-1})_a}{p} \right] \frac{1}{b^2} \left[ \frac{a(a^{-1})_a}{p} \right] \mod p \]

(7)

Our proof of the Voronoi congruence leads to a generalization modulo \( p^2 \) which has a different form than the one of Johnson (see Theorem 8 of [4]). We take the same assumptions on \( i \) as before, except when \( i \) is even (resp odd), we add the assumption that \( i \) is incongruent to 2 (resp 3) modulo \((p - 1)\). Our result is the following.

**Theorem 2.** Let \( i \) be a positive integer that is prime to \( p \).

(i) Suppose \( i \) is even and \( i \) is incongruent to 2 modulo \((p - 1)\). Then, we have:

\[
(a^i - 1)B_i = \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-1} + p \left( \frac{i - 1}{2} \right) a^{i-2} \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] b^{i-2} \mod p^2
\]

(8)
(ii) Suppose $i$ is odd and $i$ is incongruent to 1 or 3 modulo $(p - 1)$. Then, we have:

$$B_{i-1}(a^i - 1) = 2 \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-1} (ab)_0^{i-2} + (i - 1) \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-3} \mod p^2$$

$$+ p \frac{(i - 1)(i - 2)}{3} \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-3} \mod p^3$$

(9)

**Proof.** It is simply a matter of working modulo $p^3$ in the case when $i$ even and modulo $p^4$ in the case when $i$ is odd, after noticing that $\left( \frac{b}{a} \right)_2 = 0$. It yields (8) in the case when $i$ is even and

$$\frac{p}{2} B_{i-1}(a^i - 1) = \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-1} + \frac{p}{2} (i - 1) \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-2}$$

$$+ p^2 \frac{(i - 1)(i - 2)}{6} \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-3} \mod p^3$$

(10)

in the case when $i$ is odd. The first member of the right hand side of (10) is divisible by $p$ by (5) since we have assumed that $i$ is incongruent to 1 modulo $(p - 1)$. We obtain (9).

Instead of (8), Johnson’s congruence reads:

$$(a^i - 1)B_i = \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-1} - p - \frac{1}{2} a^i - 2 \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] b^{i-2} \mod p^2$$

(11)

Johnson’s sharpening of the Voronoi congruence uses the Teichmüller characters while our proof is only based on congruences concerning sums of powers of the first $(p - 1)$ integers.

Up to the sign, the second term of the right hand side of (11) is identical to the one of (8). By comparing both congruences, we derive an additional statement.

**Corollary 1.** Let $i$ be a positive even integer that is prime to $p$ and incongruent to 2 modulo $(p - 1)$. Let $a$ be an integer with $2 \leq a \leq p - 1$. Then we have:

$$2(a^i - 1)B_i = \sum_{b=1}^{p-1} \left[ \frac{ab}{p} \right] (ab)_0^{i-1} + (ab)_0^{i-1} \mod p^2$$

(12)

The next part is concerned with base 2.
3 Specificity of base 2 and related developments

A lot more studies were made in base 2. There even exists a combinatorial interpretation for the residue of the Fermat quotient in base 2. This residue relates to the number of permutations of the symmetric group $\text{Sym}(p - 2)$ with an even number of ascents, denoted for convenience by $N_{p-2}$. It is shown in [13] that

$$q_2 = (2N_{p-2})_0 - 1 \mod p$$

(13)

Thus, $p$ is a Wieferich prime if and only if the residue of twice the number of permutations of $\text{Sym}(p - 2)$ with an even number of ascents is 1.

In this part we prove two statements that are both in connection to the general case discussed in § 2. The first statement is directly linked to Theorem 1 and concerns the residue of a sum of squared powers of the first $\frac{p-1}{2}$ reciprocals.

We provide a different proof than Zhi-Hong Sun’s that the residue of the first generalized harmonic number of order $\frac{p-1}{2}$ is zero.

Proposition 1.

$$H_{\frac{p-1}{2}} = \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^2} = 0 \mod p$$

It had been known since Wolstenholme [27] that when the order of the sum is rather $(p - 1)$, this residue is zero, a result which got later generalized by Bayat to all the other generalized harmonic numbers of that order [1]. Sun’s result listed as his Corollary 5 in [19] is much more general than the single case described above, as it deals with the other generalized harmonic numbers of order $\frac{p-1}{2}$ as well, including the odd powers and also working modulo $p^2$. Contrary to what happens with the even powers, when the powers are odd, the considered residue is not zero, starting with the harmonic number of order $\frac{p-1}{2}$ whose study goes back to the work of Eisenstein from 1850. Eisenstein relates modulo $p$ the Fermat quotient in base 2 with the alternating harmonic sum of order $p - 1$ [4]:

$$q_2 = \frac{1}{2} \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \mod p$$

From Eisenstein’s formula and Wolstenholme’s theorem we easily derive:

$$H_{\frac{p-1}{2}} = \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k} = -2q_2 \mod p$$

(14)

If we denote by $H'_{p-1}$ the harmonic sum of order $p - 1$ taken only on the odd integers, we have by Eisenstein’s formula and Wolstenholme’s theorem:

$$H'_{p-1} = q_2 \mod p$$
We note that Glaisher [6] and Sun [19] a century later successively extended the expansion for \( H_{p-1}' \) to the respective moduli \( p^2 \) and \( p^3 \). Sun’s congruence reads:

\[
H_{p-1}' = q_2 - \frac{1}{2} pq_2^2 + \frac{1}{3} p^2 q_2^3 - \frac{1}{24} p^2 B_{p-3} \mod p^3
\]  

(15)

Congruence (14) is a special case of Lerch’s formula dating from 1905 which asserts, written in the Vandiver form, that:

\[
-aq_a = \sum_{u=1}^{a-1} \left( \frac{up}{a} \right) \sum_{k=1}^1 \frac{1}{k} \mod p
\]

A proof of the latter formula appears for instance in [22].

The proof of Proposition 1 goes as follows. We apply Theorem 1 with \( a = (2^{-1})_0 \). We recall from [14] that

\[
(2^{-1})_0 = \frac{p + 1}{2}
\]

This is the first expansion of Lemma 2 of [14]. Then,

\[
\left[ \frac{2(2^{-1})_0}{p} \right] = \left[ \frac{p + 1}{p} \right] = 1
\]

Moreover, if \( b \leq \frac{p-1}{2} \), then \( \left[ \frac{2b}{p} \right] = 0 \). The other \( b \)'s to the exception of \( (2^{-1})_0 = \frac{p+1}{2} \) may be written as \( p - k \) with \( k \) varying from 1 to \( \frac{p-3}{2} \). For those \( k \)'s, we have \( 3 \leq p - 2k \leq p - 2 \). Then,

\[
\left[ \frac{2(p-k)}{p} \right] = 1
\]

It follows that

\[
q_{(2^{-1})_0} = -\frac{1}{2} - 4 - \frac{p-3}{2} + 2^{-1} \sum_{k=1}^{\frac{p-3}{2}} \frac{1}{k} - (2^{-1})^2 \sum_{k=1}^{\frac{p-3}{2}} \frac{1}{k^2} \mod p,
\]

(16)

which can be rewritten using Congruence (14) as:

\[
q_{(2^{-1})_0} + q_2 = -1 - (2^{-1})^2 H_{2,\frac{p+1}{2}} \mod p
\]

(17)

Further, by a classical identity on Fermat quotients, we have:

\[
q_{(2^{-1})_0} + q_2 = q_{2,(2^{-1})_0} = q_{p+1} = -1 \mod p
\]

The result of Proposition 1 follows.
Remark 1. Doing $a = (2^{-1})_0$ in Congruence (5) leads to

\[
2^i B_i - B_i = \sum_{b=1}^{p-1} \left( \frac{2b}{p} \right) (2b)^{i-1} \mod p \quad (18)
\]

\[
= \sum_{k=1}^{p-1} 2^{i-1} (p-k)^{i-1} \mod p \quad (19)
\]

\[
= (-1)^{i-1} \sum_{k=1}^{p-1} k^{i-1} \mod p \quad (20)
\]

\[
= (-1)^i \sum_{k=1}^{p-2} k^{i-1} \mod p \quad (21)
\]

In particular, we have for every positive integer $i$ even or odd, prime to $p$ and incongruent to 1 modulo $(p-1)$:

\[
1^{i-1} + 3^{i-1} + \cdots + (p-2)^{i-1} = (2^i - 1)B_i \mod p \quad (22)
\]

Remark 2. There also exists a congruence for the odd reciprocals. Indeed, by Corollary 5.2 of [17], we know that $(p > 5)$:

\[
\sum_{k=1}^{p-1} \frac{1}{k^i} = \begin{cases} 
(2^i - 2)B_{p-i} \mod p & \text{if } i \in \{3, 5, \ldots, p-4\} \\
0 & \text{if } i \in \{2, 4, \ldots, p-5\} 
\end{cases} \quad (23)
\]

Then, we have:

\[
\frac{1}{1^{i-1}} + \frac{1}{3^{i-1}} + \frac{1}{5^{i-1}} + \cdots + \frac{1}{(p-2)^{i-1}} = \begin{cases} 
g_2 & \text{if } i = 2 \\
\left( \frac{q_2}{p-2} - 1 \right)B_{p+1-i} \mod p & \text{if } i = 4, 6, \ldots, p-3 \\
0 & \text{if } i = 3, 5, \ldots, p-4
\end{cases} \quad (24)
\]

Congruence (20) has a refinement modulo $p^2$ when $i$ is even. D. Mirimanoff has shown in [17] that the same congruence holds modulo $p^2$ under the additional condition that $i$ is incongruent to 2 modulo $(p-1)$. Independently, E. Lehmer showed in [12] a congruence modulo $p^2$ for the odd $i$’s. We gather both of their results below, with a minor change of indices $k = i - 1$ with respect to their respective original statements. In [13] we gave a common proof for both congruences. This proof is independent from the Voronoi type congruences and uses the Bernoulli polynomials.

8
### Result 3. Lehmer–Mirimanoff congruences. Let $i$ be prime to $p$ and $p-1 \nmid i-2$. Then,

\[
\sum_{r=1}^{p-1} r^{i-1} = \begin{cases} 
(2^{-i+2} - 1)B_{i-1} \frac{p}{2} \mod p^2 & \text{if } i \text{ is odd } (I)_i \\
\left(\frac{1}{2^i} - 1\right)2B_i \mod p^2 & \text{if } i \text{ is even } (II)_i 
\end{cases}
\] (25)

### Remark 3. The fact that Congruence (20) holds modulo $p^2$ under the assumptions on $i$ that $i$ is even, both $i$ and $i-1$ are prime to $p$ and $i$ incongruent to 2 modulo $(p-1)$ can be seen from Theorem 2 (i) applied in base 2. Indeed, when $a = 2$, Congruence (8) reads:

\[
(2^i - 1)B_i = \sum_{k=1}^{i} (p - 2k)^{i-1} + p \frac{i-1}{2} \frac{2^{i-2}}{2} \sum_{k=1}^{i} (p - k)^{i-2} \mod p^2
\] (26)

Further, since $i - 2$ is even, (20) itself imposes that the second sum to the right hand side of (26) is divisible by $p$ (applying (20) with odd $i - 1$ licit since $i - 1 \neq 1 \mod (p - 1)$ and $i \neq 1 \mod p$ by assumption on $i$). The latter fact may also be used inside the first sum. Therefore, (20) also holds modulo $p^2$ when $i$ is even, $i$ and $i - 1$ are prime to $p$ and $i$ is incongruent to 2 modulo $(p - 1)$, that is Mirimanoff’s congruence $(II)_i$ holds.

Lehmer’s congruence $(I)_i$ can also be deduced from a weaker form of Theorem 2 (ii) in some cases as well, namely $i$ is odd, both $i$ and $i - 1$ are relatively prime to $p$ and $i$ is incongruent to 1 modulo $(p - 1)$ (Congruence (10) is then only needed modulo $p^2$). Further, we show that $(I)_i$ has an identical refinement modulo $p^3$ under the conditions on $i$ expressed below.

### Proposition 2. Let $i$ be an odd integer with $i$ incongruent to 0 or 1 or 2 modulo $p$ and $i$ incongruent to 1 or 3 modulo $(p - 1)$.

Then the Lehmer congruence $(I)_i$ holds modulo $p^3$.

### Proof. An application of Congruence (9) with $a = 2$ under the conditions of application on $i$, that is $i$ is odd, $i$ is prime to $p$ and incongruent to 1 and 3 modulo $(p - 1)$, yields:

\[
B_{i-1}(2^i - 1) = 2 \sum_{k=1}^{i-1} \frac{(p - 2k)^{i-1}}{p} - (i - 1)2^{i-2} \sum_{k=1}^{i-1} k^{i-2} \mod p^2
\] (27)

We omitted to write the last sum of (9) as it is divisible by $p$ by the original congruence (20) applied with odd $(i - 2)$ whose application is licit since $i - 2 \neq 1 \mod (p - 1)$ and $i \neq 2 \mod p$.

Expanding the first sum to the right hand side of (27) now yields:

\[
\frac{\sum_{k=1}^{i-1} k^{i-1}}{p} = B_{i-1} \left(1 - \frac{1}{2^i}\right) + \frac{3(i-1)}{4} \sum_{k=1}^{i-1} k^{i-2} \mod p^2
\] (28)
By assumption, $i - 1$ is even, $i \neq 1 \mod p$ and $i - 1 \neq 2 \mod (p - 1)$. Then, $(II)_{i-1}$ applies. It yields:

$$\sum_{k=1}^{\frac{p-1}{2}} k^{i-2} = \left( \frac{1}{2^{i-1}} - 1 \right) 2B_{i-1} \mod p^2$$  

(29)

The result then follows from gathering Congruences (28) and (29).

□

Remark 4. The method of [13] allows to generalize such congruences modulo the other $p^r$ with $r \geq 4$ as well.

We now apply again Theorem 2 (ii) under its conditions of application on $i$ and further impose that both $i - 1$ and $i - 2$ are relatively prime to $p$. It comes:

$$pB_{i-1}2^i = pB_{i-1} + 2\sum_{k=1}^{\frac{p-1}{2}} (p - 2k)^{i-1} - p(i - 1)2^{i-2} \sum_{k=1}^{\frac{p-1}{2}} k^{i-2} \mod p^3$$  

(30)

Like before, the last sum of (9) is divisible by $p$ and thus vanishes from the congruence. This time, contrary to before, we do not expand the first sum. But we treat the second sum just like before, using Congruence (29). After regrouping the different terms we obtain:

$$pB_{i-1} = \frac{1}{2^{i-2}} \sum_{k=1}^{\frac{p-1}{2}} (p - 2k)^{i-1} \mod p^3$$  

(31)

This congruence was originally proven by Emma Lehmer in [12]. Her assumptions are weaker than ours: she only assumes that $i$ is odd and incongruent to $3$ modulo $(p - 1)$.

Email: clairelevaillant@yahoo.fr

References

[1] M. Bayat, A generalization of Wolstenholme theorem, Amer. Math. Monthly 104 (1997) 557 – 560
[2] N.G.W.H. Beeger, On a new case of the congruence $2^{p-1} = 1 (mod p^2)$, Messenger of Mathematics 51 (1922) 149 – 150
[3] T. Clausen, Theorem, Astronomische Nachrichten 17 (1840) (22) 351 – 352
[4] G. Eisenstein, Eine neue Gattung zahlentheorischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden, Berichte Königl. PreußAkad. Wiss. Berlin 15 (1850) 36 – 42 (in German)
[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 \( p^3 \), Quarterly J. Math. 31 (1900) 321 – 353

[6] J.W.L. Glaisher, On the residues of \( r^{p-1} \) to the modulus \( p^2 \), \( p^3 \) etc., Quarterly J. Math. 31 1900 – 1901 1 – 27

[7] F. Gouvea, \( p \)-adic numbers, An introduction, Second Edition, Springer 1993

[8] A. Granville and M.B. Monagan, The first case of Fermat’s last theorem is true for all prime exponents up to 714, 591, 416, 091, 389, Trans. Amer. Math. Soc. 306 (1) (1988) 329 – 359

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

[10] W. Johnson, On the nonvanishing of Fermat quotients (mod \( p \)), J. Reine und Angew. Math. Vol. 292 (1977) 196 – 200

[11] E.E. Kümmer, Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung \( z^\lambda + y^\lambda = z^\lambda \) durch ganze Zahlen unlöschbar ist, für alle diejenigen Potenz-Exponenten \( \lambda \), welche ungerade Primzahlen sind und in den Zählern der ersten \( \frac{\lambda}{2} \) Bernoullischen Zahlen als Faktoren nicht vorkommen, J. Reine und Angew. Math. 40 131 – 138 (in German)

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

[13] C. Levaillant, Powers of two weighted sum of the first \( p \) divided Bernoulli numbers modulo \( p \), preprint 2020, arXiv:2001.03471

[14] C. Levaillant, Multiple harmonic sums \( \mathcal{H}_{\{s\}=1}^{p-1} \) modulo \( p^4 \) and applications, preprint 2021, arXiv:2104.12264

[15] C. Levaillant, Some implications of the Gessel identity, preprint 2021, arXiv:2108.10553

[16] W. Meissner, Über die Teilbarkeit von \( 2^p - 2 \) durch das Quadrat der Primzahl \( p = 1093 \), Sitzungsberichte der Königl Preussischen Akademie der Wissenschaften (1913) Berlin, Zweiter Halbband, Juli bis Dezember: 663 – 667 (in German)

[17] D. Mirimanoff, Sur la congruence \( (r^{p-1} - 1) \cdot p \equiv q_r \ (mod p) \), J. Reine und Angew. Math. 115 (1895) 295 – 300 (in French)

[18] D. Mirimanoff, Sur le dernier théorème de Fermat, Comptes Rendus de l’Académie des Sciences 150 (1910) 204 – 206 (in French)

[19] Z-H. Sun, Congruences concerning Bernoulli numbers and Bernoulli polynomials, Discrete Applied Math. 105 (2000) 193 – 223
[20] J. Suzuki, On the generalized Wieferich criteria, Proceedings of the Japan Academy, Series A 70 (1994) (7):230-234

[21] H.S. Vandiver, Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat’s last theorem, J. Reine und Angew. Math. 144 (1914) 314 – 318

[22] H.S. Vandiver, Symmetric functions formed by systems of elements of a finite algebra and their connection with Fermat’s quotient and Bernoulli numbers, Ann. Math. Vol 18 No. 3 (1917) 105 – 114

[23] H.S. Vandiver, On Bernoulli numbers and Fermat’s last theorem, Duke Math. J. 3 (1937) 569 – 584

[24] C. Von Staudt, Beweis eines Lehrratzes, die Bernoullischen Zahlen betreffend, J. Reine und Angew. Math. 21 (1840) 372 – 374

[25] G.F. Voronoi, On Bernoulli numbers, Comm. Charkov Math. Soc. 2 (1890) 129 – 148 (in Russian)

[26] A. Wieferich, Zum letzen Fermatschen Theorem, J. Reine und Angew. Math. 136 (1909) 293 – 302 (in German)

[27] J. Wolstenholme, On certain properties of prime numbers, Quaterly J. Pure and Applied Math. Vol 5 (1862) 35 – 39