#A87 INTEGERS 24 (2024)

WILSON'S THEOREM MODULO p^2 DERIVED FROM FAULHABER POLYNOMIALS

Claire Levaillant
Department of Mathematics, University of Southern California, Los Angeles, California
levailla@usc.edu

Received: 4/25/23, Revised: 5/16/24, Accepted: 9/19/24, Published: 10/9/24

Abstract

First, we present a new proof of Glaisher's formula dating from 1900 and concerning Wilson's theorem modulo p^2. Our proof uses p-adic numbers and Faulhaber's formula for the sums of powers (dating back to the 17th century), as well as more recent results on Faulhaber's coefficients obtained by Gessel and Viennot. Second, by using our method, we find a simpler proof than Sun's proof regarding a formula for $(p-1)!$ modulo p^3, and one that can be generalized to higher powers of p.

1. Introduction

For p a prime number, Wilson's theorem states that

$$(p-1)! \equiv -1 \pmod{p}.$$

While there exist lots of proofs for Wilson's theorem, much less has been done regarding Wilson's theorem modulo p^2 or higher powers. It is mentioned at the end of [9] that there is no simple function of p defining the integer n_1 such that $(p-1)! \equiv -1 + n_1 p \pmod{p^2}$. In [11], Wilson's theorem modulo p^2 is only stated as

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

However, British mathematician J.W.L. Glaisher found a formula for $(p-1)! \bmod p^2$ in 1900 [7] that uses Bernoulli numbers. A hundred years later, in 2000, Z-H Sun provided a different perspective [17]. His method even allowed him to compute $(p-1)! \pmod{p^3}$, thus generalizing Glaisher's result, whose work had only led to a formula for $(p-1)! \pmod{p^2}$. Sun's result modulo p^3 is expressed in terms of divided Bernoulli numbers. We outline Sun's method below.

DOI: 10.5281/zenodo.13909158

First, he determines the generalized harmonic numbers $H_{p-1,k}$ modulo p^3. For that, he uses a battery of tools, including:

1. Euler's theorem;
2. Bernoulli's formula for the sums of powers modulo p^3;
3. The von Staudt–Clausen theorem [19][2] which determines the fractional part of Bernoulli numbers;
4. An unpublished result of [18] providing formulas for $p\,B_{k(p-1)}$ modulo p^2 and p^3 respectively, for $k = p-2$ and $k = p-1$;
5. Some generalizations modulo p^2 [17] of the Kummer congruences [14] by Sun himself.

Second, he uses Newton's formulas, together with Bernoulli's formula modulo p^2, in order to derive the Stirling numbers modulo p^2. From there, he obtains in particular a congruence for $(p-1)! \bmod p^3$ that was first proven by Carlitz [1]. Likewise, by using Newton's formulas with generalized harmonic numbers and what Sun denotes as the conjugates of the Stirling numbers, he finds a formula for the conjugate Stirling numbers modulo p^2, followed by a "conjugate Carlitz congruence". By combining the various identities, he then derives a pioneering formula for $(p-1)! \bmod p^3$, that is expressed only in terms of Bernoulli numbers.

In this paper, we provide new proofs for the generalization of Wilson's theorem to each modulus p^2 and p^3. Contrary to each of Glaisher's and Sun's earlier works, our method generalizes to higher moduli. This is one of the reasons to present it here.

The paper arose from an analogy between two polynomials f and g defined as

$$\begin{cases} f = X^{p-1} - 1 \in \mathbb{Z}/p\,\mathbb{Z}[X] \\ g = X^{p-1} + (p-1)! \in \mathbb{Z}_p[X], \end{cases}$$

where p is a prime number, $\mathbb{Z}/p\,\mathbb{Z}$ denotes the field with p elements, and $\mathbb{Z}_p$ denotes the ring of p-adic integers; see [8]. The analogy is concerned with the way each polynomial factors and with the congruence properties that can be derived in each case from the relations between the coefficients and the roots.

We first investigate the factorization of f and the properties modulo p that can be derived from it. By Fermat's little theorem we have,

$$k^{p-1} = 1 \text{ in } \mathbb{Z}/p\,\mathbb{Z},$$

for all integers k with $1 \leq k \leq p-1$. This provides the $(p-1)$ roots of f, and so f factors in $\mathbb{Z}/p\,\mathbb{Z}[X]$ as

$$f = (X-1)(X-2)\dots(X-(p-1)).$$

From looking at the constant coefficient of f in both factored and expanded forms, we retrieve Wilson's theorem. This constitutes one of many proofs for Wilson's theorem. By looking at the other coefficients in both factored and expanded forms, we derive more divisibility relations. Namely, for all integers k where $2 \leq k \leq p-1$, we have that p divides $\left[\begin{matrix} p \\ k \end{matrix} \right]$. The latter numbers, referred to as *unsigned Stirling numbers of the first kind*, are the respective unsigned coefficients of $x^2, x^3, \ldots, x^{r+1}, \ldots, x^{p-1}$ in the falling factorial

$$x(x-1)(x-2)\ldots(x-(p-1)).$$

It is a well known fact that these numbers also count the number of permutations of p elements that decompose into a product of k disjoint cycles.

Similarly, we now investigate the factorization of g. Let k be an integer with $1 \leq k \leq p-1$. First, we have

$$g(k) = k^{p-1} + (p-1)! \in p\,\mathbb{Z}_p, \tag{1}$$

by definition of g and by using Wilson's theorem modulo p. Moreover, we have

$$g^{'}(k) = (p-1)\,k^{p-2} \notin p\,\mathbb{Z}_p, \tag{2}$$

as $k^{p-2} = k^{-1} \neq 0$ in $\mathbb{Z}/p\,\mathbb{Z}$. Hence, by Hensel's lemma [8], each nonzero k of $\mathbb{Z}/p\,\mathbb{Z}$ lifts to a unique root x_k of g such that $k - x_k \in p\,\mathbb{Z}_p$. Let $x_k = k + p\,t_k$, with $t_k \in \mathbb{Z}_p$. Then g factors in $\mathbb{Z}_p[X]$ as follows,

$$g = (X - 1 - p\,t_1)\ldots\,(X - (p-1) - p\,t_{p-1}).$$

We will see that, by looking at the constant coefficient of g modulo $p^2\,\mathbb{Z}_p$, we are able to p-adically expand $(p-1)!$ further. Our result is the following.

Theorem 1. *Let $\delta_0(k)$ be defined for each integer k with $1 \leq k \leq p-1$ by*

$$k^{p-1} \equiv 1 + p\,\delta_0(k) \pmod{p^2}.$$

Then, the following congruence holds:

$$(p-1)! \equiv -1 + p\sum_{k=1}^{p-1} \delta_0(k) \pmod{p^2}.$$

By working out the sum of Theorem 1 modulo p^2 using the Faulhaber polynomials for the sums of powers of integers and by using Faulhaber's neat statement on the relationship between the two trailing coefficients of the polynomial for the odd powers (work done in the 17th century [5]), we obtain Wilson's theorem one step further, namely modulo p^2.

Theorem 2. *Let p be an odd prime number. Set $p = 2l + 1$ and $a = \frac{p(p-1)}{2}$. Let $c_1(l)$ be the trailing coefficient in the Faulhaber polynomial:*

$$\sum_{k=1}^{p-1} k^p = c_l(l)\, a^{l+1} + \ldots + c_2(l)\, a^3 + c_1(l)\, a^2. \tag{3}$$

We have,

$$(i)\ \textit{for all}\ i \in \{1, \ldots, l\},\ c_i(l) \in \mathbb{Z}_p\,;$$

$$(ii)\ (p-1)! \equiv \tfrac{1}{2}\, c_1(l) - p \pmod{p^2}.$$

Corollary 1 (Wilson's theorem modulo p^2, [7])**.** *Let p be a prime number and let B_{p-1} denote the Bernoulli number of order $(p-1)$. The following congruence holds:*

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

Wilson's theorem modulo p^2 was originally stated by Glaisher. Contrary to our proof, his proof involves first finding the unsigned Stirling numbers of the first kind modulo p^2. Also, Glaisher's method does not generalize to the modulus p^3, while ours does. Namely, Theorem 1 has a generalization to the modulus p^3, as follows.

Theorem 3. *Let $\delta_1(k)$ denote the third residue in the p-adic expansion of k^{p-1}, namely:*

$$k^{p-1} \equiv 1 + p\, \delta_0(k) + p^2\, \delta_1(k) \pmod{p^3}. \tag{4}$$

Then, the following congruence holds:

$$\begin{aligned}(p-1)! \equiv -1 + p \sum_{i=1}^{p-1} \delta_0(i) + p^2 \sum_{i=1}^{p-1} \Big(\delta_0(i) + \delta_1(i)\Big) \\ - \frac{p^2}{2}\left[\Big(\sum_{i=1}^{p-1} \delta_0(i)\Big)^2 + \sum_{i=1}^{p-1} \delta_0(i)^2\right] \pmod{p^3}.\end{aligned} \tag{5}$$

From there, it is easily seen that $(p-1)!$ modulo p^3 can be written in terms of sums of powers, and powers of sums of powers. We then derive a congruence for $(p-1)!$ modulo p^3 in terms of Bernoulli numbers.

Corollary 2. *We have*

$$(p-1)! \equiv \frac{p}{2} - \frac{3}{2}p^2 + (2p+1)pB_{p-1} - \frac{1}{2}p\, B_{2p-2} - \frac{1}{2}\, p^2\, B_{p-1}^2 \pmod{p^3}. \tag{6}$$

We further show that this congruence, though of different expression, is equivalent to the congruence obtained by Z-H. Sun in [17]. Again, our method can be generalized to higher moduli, while Sun's method does not apply to higher moduli.

The paper is divided into two parts, namely one presenting a proof of Wilson's theorem modulo p^2 and one presenting a proof of Wilson's theorem modulo p^3.

2. A Proof of Wilson's Theorem Modulo p^2

We recall that the polynomial $g = X^{p-1} + (p-1)! \in \mathbb{Z}_p[X]$ factors as

$$g = (X - 1 - p\,t_1) \dots (X - (p-1) - p\,t_{p-1}).$$

In this part, we will work out the constant coefficient of the polynomial g modulo $p^2\,\mathbb{Z}_p$, using both the factored form and the expanded form of g. This will lead to the formula of Theorem 1. To that end, we will first need to investigate the p-residues of the t_k's. For $1 \leq, k \leq p-1$, we will denote the p-residue of t_k by $t_k^{(0)}$. Using Hensel's lifting algorithm, we show the following result.

Lemma 1. *Let k be an integer with $1 \leq k \leq p-1$. Then, we have*

$$p\,t_k^{(0)} \equiv k(1 + (p-1)! + p\,\delta_0(k)) \pmod{p^2}. \tag{7}$$

Here, $\delta_0(k)$ is defined as in the statement of Theorem 1; see Section 1.

Proof. We recall from the introduction that $k \in \mathbb{Z}/p\,\mathbb{Z}$ lifts to a unique root $k + pt_k$ of g, with t_k a p-adic integer. According to Hensel's lifting algorithm, the second coefficient $t_k^{(0)}$ of the root expansion must satisfy

$$g(k + p\,t_k^{(0)}) \in\, p^2\mathbb{Z}_p.$$

Hence, we must have

$$k^{p-1} + p(p-1)t_k^{(0)}\,k^{p-2} + (p-1)! \in p^2\mathbb{Z}_p. \tag{8}$$

But,

$$k^{p-1} \equiv 1 + p\delta_0(k) \pmod{p^2}.$$

And so,

$$k^{p-2} \equiv k^{-1} + p\delta_0(k)\,k^{-1} \pmod{p^2}.$$

Plugging the latter congruence into (8) and reducing modulo p^2 yields the congruence of Lemma 1. □

Before moving any further, we will introduce some notation for the divided factorials. Let r be an integer with $1 \leq r \leq p-2$ and let $i_1, i_2, \dots, i_r$ be r integers with $1 \leq i_k \leq p-1$ for all k with $1 \leq k \leq r$. We define the *divided factorial* $(p-1)!^{i_1,\dots,i_r}$ as

$$(p-1)!^{i_1,\dots,i_r} := \frac{(p-1)!}{\prod_{k=1}^{r} i_k}.$$

With Lemma 1, we are ready to prove Theorem 1, as follows.

Proof of Theorem 1. By looking at the constant coefficient of g modulo p^2, we obtain

$$\sum_{k=1}^{p-1} pt_k^{(0)}(p-1)!^k \equiv 0 \pmod{p^2}. \tag{9}$$

Then, by using Lemma 1, we get

$$(p-1)!\sum_{k=1}^{p-1}(1+(p-1)!+p\delta_0(k)) \equiv 0 \pmod{p^2}. \tag{10}$$

We further derive

$$(p-1)!\Big((p-1)(1+(p-1)!)+p\sum_{k=1}^{p-1}\delta_0(k)\Big) \equiv 0 \pmod{p^2}. \tag{11}$$

By using Wilson's theorem modulo p inside the bracket, we derive in turn

$$(p-1)!\Big(-1-(p-1)!+p\sum_{k=1}^{p-1}\delta_0(k)\Big) \equiv 0 \pmod{p^2}. \tag{12}$$

Finally, since p^2 and $(p-1)!$ are relatively prime, we obtain the congruence of Theorem 1. □

Using some of Faulhaber's mathematics, we can now prove Theorem 2.

Proof of Theorem 2. First of all, Congruence (12) can be written in terms of a sum of powers of integers as follows:

$$(p-1)! \equiv -p+\sum_{k=1}^{p-1}k^{p-1} \pmod{p^2}. \tag{13}$$

Sums of powers of integers were first studied by Faulhaber in 1631 [5]. He had noticed that the sum of a fixed odd power of the first n integers is a polynomial in $a=\frac{n(n+1)}{2}$ of the form

$$\sum_{k=1}^{n}k^{2m+1} = c_1(m)a^2+c_2(m)a^3+\cdots+c_m(m)a^{m+1}. \tag{14}$$

It was not until 1834 that his formula was given a rigorous proof, by Jacobi; see [12]. Faulhaber's formula for the even powers can be obtained from his formula for the odd powers and reads

$$\sum_{k=1}^{n}k^{2m} = \frac{n+\frac{1}{2}}{2m+1}(2c_1(m)a+3c_2(m)a^2+\cdots+(m+1)c_m(m)a^m).$$

Assume point (i) of Theorem 2 holds. Then, by using Faulhaber's formula for sums of even powers $2l$ of the first n integers with $2l = p-1$ and $n = p-1$, we get

$$p\sum_{k=1}^{p-1} k^{p-1} \equiv \Big(p-1+\frac{1}{2}\Big)\Big(2\,c_1(l)\frac{p(p-1)}{2} + 3\,c_2(l)\frac{p^2(p-1)^2}{4}\Big) \pmod{p^3}. \tag{15}$$

Further, back in the 17th century, Faulhaber states that the two trailing coefficients in Equation (14) will have the form $4\alpha\, a^3 - \alpha\, a^2$. By using this fact and simplifying, we obtain

$$\sum_{k=1}^{p-1} k^{p-1} \equiv \frac{1}{2}c_1(l) \pmod{p^2}. \tag{16}$$

Combining Congruences (13) and (16) leads to Congruence (ii) of Theorem 2.

It remains to show (i). The starting point is Jacobi's formula [12]. Using our notation for a and letting $u = 2a$, Jacobi's formula reads

$$\sum_{k=1}^{p-1} k^{2l+1} = \frac{1}{p+1}\Big(A_0^{(l+1)}\,u^{l+1} + A_1^{(l+1)}\,u^{l} + \cdots + A_l^{(l+1)}\,u\Big). \tag{17}$$

In the most general form of the formula, the denominator $p+1$ should be replaced with $2l+2$. Confronting Jacobi's formula with Faulhaber's formula in Equation (3), we see that

$$A_l^{(l+1)} = 0 \qquad \text{and} \qquad c_i(l) = \frac{2^{i+1}\,A_{l-i}^{(l+1)}}{p+1}. \tag{18}$$

It is known that the coefficients $A_k^{(m)}$ obey some recurrence formulas. Moreover, an explicit formula for these coefficients was first obtained by Gessel and Viennot in [6] and is provided by Knuth in [13]. Further, Edwards was the first to observe from a recursive formula defining the $A_k^{(m)}$'s and involving binomial coefficients, that these numbers can be obtained by inverting a lower triangular matrix; see [4]. From there, Gessel and Viennot expressed the coefficients in terms of a $k \times k$ determinant, namely

$$A_k^{(m)} = \frac{1}{(1-m)\dots(k-m)}\begin{vmatrix} \binom{m-k+1}{3} & \binom{m-k+1}{1} & 0 & \dots & 0 \\ \binom{m-k+2}{5} & \binom{m-k+2}{3} & \binom{m-k+2}{1} & \dots & 0 \\ \vdots & \vdots & \vdots & & \\ \binom{m-1}{2k-1} & \binom{m-1}{2k-3} & \binom{m-1}{2k-5} & \dots & \binom{m-1}{1} \\ \binom{m}{2k+1} & \binom{m}{2k-1} & \binom{m}{2k-3} & \dots & \binom{m}{3} \end{vmatrix}.$$

Of interest here, we note that this determinant is an integer. In fact, this determinant has a neat combinatorial interpretation that is due to Gessel and Viennot. A result in [6] states that this determinant counts the number of ways to put positive integers into a k-rowed tripled staircase, with numbers strictly increasing from left to right and from top to bottom, and imposing also that an entry in row j is at most $m-k+j$; see Figure 1.

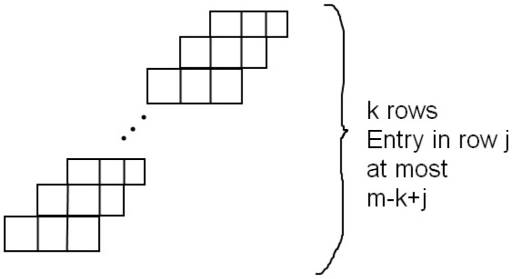

Figure 1.

Our goal is to show that $c_i(l) \in \mathbb{Z}_p$. For that, we use Formula (18). From the discussion above, we know that

$$A_{l-i}^{(l+1)} = \frac{1}{l(l-1)(l-2)\dots(l-(l-i-1))} \times s,$$

for some integer s. Now $l = \frac{p-1}{2} < p$, hence p does not divide the denominator of $A_{l-i}^{(l+1)}$. Thus, $A_{l-i}^{(l+1)}$ is a p-adic integer and so is $c_i(l)$ for each i. This closes the proof of Theorem 2. □

We are now in a position to retrieve Glaisher's result from 1900, stated in the introduction as Corollary 1.

Proof of Corollary 1. It is known from [13] that

$$A_{m-2}^{(m)} = \binom{2m}{2} B_{2m-2} \text{ for all } m \geq 2,$$

with the Bernoulli numbers defined recursively by

$$B_0 = 1 \text{ and } \sum_{k=0}^{n-1} \binom{n}{k} B_k = 0, \text{ for } n > 1.$$

Hence

$$c_1(l) = \frac{4A_{l-1}^{(l+1)}}{p+1} = \frac{4p(p+1)}{2(p+1)} B_{p-1} = 2p\, B_{p-1}. \tag{19}$$

By (13), (16) and (19), we conclude that

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

This ends the proof of Corollary 1.

The method just exposed allows us to bypass the use of von Staudt-Clausen's theorem. Another way of getting Glaisher's formula directly from Theorem 1 would be to use Bernoulli's formula together with von Staudt-Clausen's theorem.

Bernoulli's formula for the sums of powers reads

$$\sum_{k=1}^{p} k^m = \frac{1}{m+1}\sum_{j=0}^{m}\binom{m+1}{j} B_j\, p^{m+1-j}, \tag{20}$$

where we write the formula using Bernoulli numbers of the second type, that is, $B_1 = \frac{1}{2}$ instead of $B_1 = -\frac{1}{2}$ and all the other Bernoulli numbers remain unchanged. Since the Bernoulli numbers with odd indices are all zero, except for B_1, this thus avoids having to carry minus signs in the original Bernoulli formula. A trick first noticed by Z-H. Sun consists of summing the $(p-1)$th powers of integers up to p, instead of $(p-1)$, since we work modulo small powers of p and the last term of the sum will not contribute anyway. This way, Bernoulli's formula can be expressed in terms of powers of p instead of powers of $(p-1)$. We get:

$$p\sum_{k=1}^{p} k^{p-1} = \sum_{j=0}^{p-1}\binom{p}{j} B_j\, p^{p-j}. \tag{21}$$

By (13), we need to know $p\sum_{k=1}^{p} k^{p-1}$ modulo p^3. This is why we need to know the p-divisibility properties of the denominators of the Bernoulli numbers. A consequence of von Staudt-Clausen's theorem is that the denominator of the Bernoulli number B_{2n} equals the product of all the primes p such that $p-1$ divides $2n$; see [2], and independently [19]. Thus, amongst the Bernoulli numbers present in the sum of Equation (21), the prime p divides the denominator of only B_{p-1}. We thus deduce

$$\sum_{k=1}^{p-1} k^{p-1} \equiv p\,B_{p-1} \pmod{p^2\mathbb{Z}_p}. \tag{22}$$

Glaisher's formula then follows from Congruences (13) and (22). □

We note from Glaisher's formula an improvement for calculating $(p-1)!$ modulo p^2. For instance, the one millionth Bernoulli number has 4767554 digits over 24 digits and the 1.5 millionth Bernoulli number has 7415484 digits over 55 digits. A work by Derby dating from 2015 has provided an efficient method for computing $p\,B_{p-1}$. In order to explain Derby's way, we must first introduce some new notation.

Denote by $\widehat{PT}(n)$ the lower triangular matrix obtained by entering the coefficients of the Pascal triangle with the ending 1 coefficient omitted.

Write

$$\begin{aligned}\sum_{k=1}^{p-1} k^p &= \frac{1}{p+1}\sum_{j=0}^{p}\binom{p+1}{j} B_j\,(p-1)^{p+1-j} \\ &= d_1(p-1)+d_2(p-1)^2+\cdots+d_{p+1}(p-1)^{p+1},\end{aligned}$$

according to Bernoulli's formula. Derby's result provides a way of computing the coefficients d_i by simply inverting a matrix involving the Pascal triangle.

Fact 1 ([3])**.** *We have*

$$(1\;p\;\ldots\;p\;1)\widehat{PT}(p+1)^{-1} = (d_1\,d_2\,\ldots\,d_{p+1}),$$

with the leftmost parenthetical expression denoting the p-th row of the Pascal triangle.

From there, since the second coefficient d_2 is

$$\frac{1}{p+1}\binom{p+1}{p-1} B_{p-1} = \frac{p}{2}\,B_{p-1},$$

it provides an efficient way of computing $(p-1)!$ modulo p^2.

For interest and completeness here, we note that work similar to Derby's, and additional results involving the sums of powers and the Pascal triangle, were achieved by Pietrocola and published electronically in 2017; see [15].

3. A Proof of Wilson's Theorem Modulo p^3

Like we did in the modulus p^2 case, we must lift the root residues of g one p-power further. First, we introduce a new notation. In what follows, the x_k's with $1 \le k \le p-1$ denote the $(p-1)$ p-adic integer roots of $g = X^{p-1}+(p-1)!$. Define $t_k^{(1)}$ as the p-adic residue such that

$$x_k \equiv k + p\,t_k^{(0)} + p^2\,t_k^{(1)} \pmod{p^3}.$$

The following lemma will be useful for the proof of Theorem 3.

Lemma 2. *We have*

$$t_k^{(1)} \equiv k\Big(\delta_0(k)+\delta_1(k)+\left(\sum_{i=1}^{p-1}\delta_0(i)\right)^2 + (1+\delta_0(k))\sum_{i=1}^{p-1}\delta_0(i)\Big) \pmod{p}.$$

Proof. Hensel's lifting algorithm imposes

$$g(k+p\,t_k^{(0)}+p^2\,t_k^{(1)}) \in\, p^3\mathbb{Z}_p,$$

that is

$$(k+p\,t_k^{(0)}+p^2\,t_k^{(1)})^{p-1}+(p-1)! \in\, p^3\mathbb{Z}_p.$$

Expanding yields

$$k^{p-1}+p(p-1)t_k^{(0)}k^{p-2}+\frac{(p-1)(p-2)}{2}p^2\big(t_k^{(0)}\big)^2k^{p-3} \\ +p^2(p-1)t_k^{(1)}(k+p\,t_k^{(0)})^{p-2}+(p-1)! \in p^3\,\mathbb{Z}_p.$$

Another round of simplifications modulo p^3 now leads to

$$k^{p-1}+p\,t_k^{(0)}(p-1)k^{p-2}-p^2t_k^{(1)}k^{p-2}+p^2\big(t_k^{(0)}\big)^2\,k^{p-3}+(p-1)! \in p^3\,\mathbb{Z}_p.$$

Notice that since $0 \le t_k^{(0)} \le p-1$, we have $t_k^{(0)} \bmod p^2 \equiv t_k^{(0)} \bmod p$. It follows that $pt_k^{(0)} \bmod p^3 \equiv p\,t_k^{(0)} \bmod p^2$. Hence we have by Lemma 1,

$$pt_k^{(0)} \equiv k(1+(p-1)!+p\,\delta_0(k)) \pmod{p^3}.$$

We thus get

$$p^2\,t_k^{(1)}\,k^{-1} \equiv k^{p-1}\Big(1+(p-1)(1+(p-1)!+p\delta_0(k))+(1+(p-1)!+p\delta_0(k))^2\Big) \\ +(p-1)! \pmod{p^3}.$$

After replacing

$$k^{p-1} \equiv 1+p\delta_0(k)+p^2\delta_1(k) \pmod{p^3},$$

using Theorem 1 when appropriate, and reducing modulo p^3, we obtain the expression of Lemma 2. □

Theorem 3 is then derived by looking at the constant coefficient of g modulo p^3 in both factored and expanded forms. The calculation gets detailed below.

Proof of Theorem 3. We have

$$(p-1)! \equiv (p-1)!+\sum_{k=1}^{p-1}p\,t_k^{(0)}\,(p-1)!^k+\sum_{k=1}^{p-1}p^2\,t_k^{(1)}(p-1)!^k \\ +\sum_{i\neq j}pt_i^{(0)}pt_j^{(0)}(p-1)!^{i,j} \pmod{p^3}.$$

Then, by factoring $(p-1)!$ and using Lemma 1 and Lemma 2, we obtain

$$\begin{aligned}(p-1)!\Bigg(&\sum_{k=1}^{p-1}(1+(p-1)!+p\delta_0(k))+p^2\sum_{k=1}^{p-1}(\delta_0(k)+\delta_1(k))\\&-p^2\left(\sum_{i=1}^{p-1}\delta_0(i)\right)^2+p^2\left(\sum_{i=1}^{p-1}\delta_0(i)\right)\sum_{k=1}^{p-1}(1+\delta_0(k))\\&+\sum_{i\neq j}\big(1+(p-1)!+p\delta_0(i)\big)\big(1+(p-1)!+p\delta_0(j)\big)\Bigg)\equiv 0 \pmod{p^3}.\end{aligned}$$

We derive,

$$\begin{aligned}(p-1)!\Bigg(&p^2\sum_{i=1}^{p-1}\delta_0(i)-1-(p-1)!+p\sum_{i=1}^{p-1}\delta_0(i)+p^2\sum_{i=1}^{p-1}(\delta_1(i)+\delta_0(i))\\&-p^2\left(\sum_{i=1}^{p-1}\delta_0(i)\right)^2-p^2\sum_{i=1}^{p-1}\delta_0(i)+p^2\left(\sum_{i=1}^{p-1}\delta_0(i)\right)^2\\&+\frac{1}{2}\sum_{i=1}^{p-1}\sum_{j\neq i}\big(1+(p-1)!+p\delta_0(i)\big)\big(1+(p-1)!+p\delta_0(j)\big)\Bigg)\equiv 0 \pmod{p^3}.\end{aligned}$$

In the left-hand side above, some terms simplify. Denote by S the double sum. We evaluate it as follows. We have

$$\begin{aligned}S\equiv\frac{1}{2}\Bigg(&\sum_{i=1}^{p-1}(1+(p-1)!+p\delta_0(i))\sum_{j=1}^{p-1}(1+(p-1)!+p\delta_0(j))\\&-\sum_{i=1}^{p-1}\Big(1+(p-1)!+p\delta_0(i)\Big)^2\Bigg) \pmod{p^3}.\end{aligned}$$

A quick inspection shows that the first term of the difference above is congruent to zero modulo p^3. Thus, modulo p^3, the double sum S reduces to

$$S\equiv-\frac{p^2}{2}\left(\left(\sum_{i=1}^{p-1}\delta_0(i)\right)^2+\sum_{i=1}^{p-1}\delta_0(i)^2\right) \pmod{p^3}.$$

By gathering the different parts, we obtain the congruence of Theorem 3. □

It remains to express $(p-1)!$ modulo p^3 in terms of sums of powers, and powers of sums of powers. From there, we will derive the congruence of Corollary 2, that is, Wilson's theorem modulo p^3. To that end, we prove the following lemma.

Lemma 3. *We have*

$$(p-1)! \equiv -1 - \frac{1}{2}\left(\left(\sum_{i=1}^{p-1} i^{p-1}\right)^2 + \sum_{i=1}^{p-1}(i^{p-1})^2\right) + (2p+1)\sum_{i=1}^{p-1} i^{p-1} \\ - (p-1)(\frac{3}{2}p+1) \pmod{p^3}.$$

Proof. We start from the congruence of Theorem 3. First, we group the terms so as to use the expansion

$$i^{p-1} \equiv 1 + p\delta_0(i) + p^2\delta_1(i) \pmod{p^3}.$$

We get,

$$(p-1)! \equiv -1 + \sum_{i=1}^{p-1}(p\delta_0(i) + p^2\delta_1(i)) + p^2\sum_{i=1}^{p-1}\delta_0(i) \\ -\frac{1}{2}\sum_{i=1}^{p-1}(i^{p-1} - 1 - p^2\delta_1(i))^2 - \frac{1}{2}\left(\sum_{i=1}^{p-1} i^{p-1} - (p-1) - p^2\sum_{i=1}^{p-1}\delta_1(i)\right)^2 \pmod{p^3}. \tag{23}$$

Denote the last two blocks of terms of (23) respectively by S_3 and S_4; that is,

$$\begin{cases} S_3 := -\frac{1}{2}\sum_{i=1}^{p-1}(i^{p-1} - 1 - p^2\delta_1(i))^2 \\ S_4 := -\frac{1}{2}\left(\sum_{i=1}^{p-1} i^{p-1} - (p-1) - p^2\sum_{i=1}^{p-1}\delta_1(i)\right)^2 \end{cases}.$$

We proceed to the evaluation of these two sums. We have, by expanding the square of S_3,

$$S_3 \equiv -\frac{1}{2}\sum_{i=1}^{p-1} i^{2p-2} - \frac{1}{2}(p-1) + \sum_{i=1}^{p-1} i^{p-1} + p^2\sum_{i=1}^{p-1}\delta_1(i)\left(i^{p-1} - 1\right) \pmod{p^3}.$$

Then, by using the expression for $p^2\delta_1(i)$ modulo p^3 and replacing,

$$S_3 \equiv -\frac{1}{2}\sum_{i=1}^{p-1} i^{2p-2} - \frac{1}{2}(p-1) + \sum_{i=1}^{p-1} i^{p-1} + \sum_{i=1}^{p-1}(i^{p-1} - 1 - p\delta_0(i))(i^{p-1} - 1) \pmod{p^3}.$$

By expanding the factor in the last sum above, and regrouping the terms, it follows that

$$S_3 \equiv \frac{1}{2}\sum_{i=1}^{p-1} i^{2p-2} + \frac{1}{2}(p-1) - \sum_{i=1}^{p-1} i^{p-1} + p\sum_{i=1}^{p-1}\delta_0(i) - p\sum_{i=1}^{p-1}\delta_0(i)i^{p-1} \pmod{p^3}.$$

From there, notice that

$$p\delta_0(i)\,p\delta_0(i) \equiv p\delta_0(i)\,(i^{p-1}-1) \pmod{p^3}.$$

Then, modulo p^3, the linear combination of the last two sums of S_3 above is nothing other than $2\,S_3$. It follows that

$$S_3 \equiv -\frac{1}{2}\sum_{i=1}^{p-1} i^{2p-2} + \sum_{i=1}^{p-1} i^{p-1} - \frac{1}{2}(p-1) \pmod{p^3}. \tag{24}$$

We now tackle S_4. First, we expand the square. It yields

$$S_4 \equiv -\frac{1}{2}\Bigg(\sum_{i=1}^{p-1} i^{p-1}\Bigg)^2 - \frac{1}{2}(p-1)^2 + (p-1)\sum_{i=1}^{p-1} i^{p-1} \\ + \Bigg(p^2\sum_{i=1}^{p-1}\delta_1(i)\Bigg)\Bigg(\sum_{i=1}^{p-1} i^{p-1} - (p-1)\Bigg) \pmod{p^3}.$$

Next, by replacing $p^2\delta_1(i)$ modulo p^3,

$$S_4 \equiv -\frac{1}{2}\Bigg(\sum_{i=1}^{p-1} i^{p-1}\Bigg)^2 - \frac{1}{2}(p-1)^2 + (p-1)\sum_{i=1}^{p-1} i^{p-1} \\ + \Bigg(\sum_{i=1}^{p-1}\big(i^{p-1}-1-p\delta_0(i)\big)\Bigg)\Bigg(\sum_{i=1}^{p-1} i^{p-1} - (p-1)\Bigg) \pmod{p^3}.$$

Expanding the last term and simplifying leads to

$$S_4 \equiv \frac{1}{2}\Bigg(\sum_{i=1}^{p-1} i^{p-1}\Bigg)^2 + \frac{1}{2}(p-1)^2 - (p-1)\sum_{i=1}^{p-1} i^{p-1} + 2\,S_4 \pmod{p^3},$$

from which we finally derive

$$S_4 \equiv -\frac{1}{2}\Bigg(\sum_{i=1}^{p-1} i^{p-1}\Bigg)^2 - \frac{1}{2}(p-1)^2 + (p-1)\sum_{i=1}^{p-1} i^{p-1} \pmod{p^3}. \tag{25}$$

By plugging the respective expressions (24) and (25) for S_3 and S_4 into (23) and simplifying, we obtain the congruence of Lemma 3. □

We finally derive Corollary 2.

Proof of Corollary 2. From Lemma 3, deriving Wilson's theorem modulo p^3 as in Corollary 2, is simply a matter of applying von Staudt-Clausen's theorem and Sun's congruence

$$S_m := \sum_{k=1}^{p-1} k^m \equiv p\,B_m + \frac{p^2}{2}\,m\,B_{m-1} + \frac{p^3}{6}\,m(m-1)\,B_{m-2} \pmod{p^3} \tag{26}$$

of [17]. Z-H. Sun derived the above congruence from a smart use of Bernoulli's formula, together with an application of von Staudt-Clausen's theorem. □

Lastly, we establish below the a priori nontrivial equivalence between our congruence and Z-H. Sun's congruence dating from 2000. Sun's formula from [17] reads

$$(p-1)! \equiv -\frac{p\,B_{p-1}}{p-1} + \frac{p\,B_{2p-2}}{2(p-1)} - \frac{1}{2}\Big(\frac{p\,B_{p-1}}{p-1}\Big)^2 \pmod{p^3}. \tag{27}$$

First, we note that

$$(p-1)^{-1} \equiv -p^2 - p - 1 \pmod{p^3}. \tag{28}$$

Next, it is a straightforward consequence of von Staudt-Clausen's theorem that

$$pB_{p-1} \equiv -1 \pmod{p\,\mathbb{Z}_p} \text{ and } pB_{2(p-1)} \equiv -1 \pmod{p\,\mathbb{Z}_p}. \tag{29}$$

Then, Sun's congruence can be rewritten as

$$(p-1)! \equiv -2p^2 - \frac{p(p+1)}{2}\,B_{2p-2} + p(p+1)\,B_{p-1} - \frac{2p+1}{2}\,p^2 B_{p-1}^2 \pmod{p^3}. \tag{30}$$

At this point, we need to expand $pB_{2(p-1)}$ one p-power further. By an unpublished result of Sun from [18], we have the following.

Proposition 1 ([18])**.** *Let k be a nonnegative integer. Then,*

$$p\,B_{k(p-1)} \equiv -(k-1)(p-1) + k\,p\,B_{p-1} \pmod{p^2}. \tag{31}$$

This statement is a special case of his more general Corollary 4.2 appearing in [16]. Applied with $k=2$, it yields

$$pB_{2(p-1)} \equiv 2pB_{p-1} - p + 1 \pmod{p^2\mathbb{Z}_p}. \tag{32}$$

We must introduce some new notation. Let x be a p-adic integer. We denote by $(x)_k$ the $(k+1)$-th p-residue in the p-adic expansion of x, that is

$$x = \sum_{j=0}^{\infty} (x)_j\, p^j.$$

Using this notation, writing

$$\begin{cases} pB_{p-1} & \equiv & p-1+p(pB_{p-1})_1 & \pmod{p^2\mathbb{Z}_p} \\ pB_{2(p-1)} & \equiv & p-1+p(pB_{2(p-1)})_1 & \pmod{p^2\mathbb{Z}_p} \end{cases},$$

and plugging back into Congruence (32), we derive:

$$(pB_{2(p-1)})_1 \equiv 2(pB_{p-1})_1 \pmod{p\,\mathbb{Z}_p}. \tag{33}$$

By using (33) in (30), we finally obtain, following a routine calculation, the formula of our Corollary 2. We conclude that Z-H. Sun's congruence and our congruence are both equivalent.

4. Conclusion

Our work involving the factorization of the polynomial $X^{p-1} + (p-1)!$ in $\mathbb{Z}_p[X]$ also allows one to find congruences for the unsigned Stirling numbers of the first kind modulo p^2 and p^3. It is interesting to note again that Glaisher's proof of Wilson's theorem modulo p^2 uses knowledge of the Stirling numbers modulo p^2, which he computes by quite original means. Thus, our method also allows us to retrieve these results, but we do not use them for proving Wilson's theorem modulo p^2. Sun's method leads to the next modulus p^3, but it involves a lot more work, like working out the generalized harmonic numbers modulo p^3. Also, his method is specific to modulus p^3 and does not generalize to modulus p^4 and higher moduli. On the contrary, our method for modulus p^3 can be generalized to higher moduli. It is based only on Hensel's lifting algorithm, and on the conjunction of Bernoulli's formula for the sums of powers of integers and von Staudt-Clausen's theorem for Bernoulli numbers.

This field has very much drawn the attention of mathematicians over several centuries and is still being researched today. A sign of the vibrant interest is that many authors have also been investigating the quantum analogs. Amongst these results, a quantum analog for Faulhaber's formula is provided by the authors in [10].

Acknowledgement. The author gratefully acknowledges the anonymous referee whose dedicated reading allowed the author to better the writing substantially. She also gratefully acknowledges the very kind formatting team, whose careful and precise reading allowed her to better the manuscript substancially.

References

[1] L. Carlitz, A theorem of Glaisher, *Canad. J. Math.* **5** (1953), 306-316.

[2] T. Clausen, Theorem, *Astron. Nachr.* **17** (22) (1840), 351-352.

[3] N. Derby, A search for sums of powers, *Math. Gaz.* **99** (546) (2015), 416-421.

[4] A. W. F. Edwards, A quick route to sums of powers, *Amer. Math. Monthly* **93** (6) (1986), 451-455.

[5] J. Faulhaber, Darinnen die miraculosische Inventiones zu den höchsten Cossen weiters continuirt und prolifiert werden, *Academia Algebrae* (1631).

[6] I. Gessel and G. Viennot, *Determinants, Paths and Plane Partition*, Brandeis University report, July 1989, unpublished, https://people.brandeis.edu/ gessel/homepage/papers/pp.pdf

[7] 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, *Quart. J. Math.* **31** (1900), 321-353.

[8] F. Gouvea, *P-adic Numbers, an Introduction*, Second Edition, Springer, 1993.

[9] D. B. Grünberg, Integrality of open instantons numbers, *J. Geom. Phys.* **52** (3) (2004), 284-297.

[10] V. J. W. Guo and J. Zeng, A q-analog of Faulhaber's formula for sums of powers, *Electron J. Combin.* **11** (2) (2004-6) (The Stanley Festschrift volume), #R19.

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, Oxford, 1979.

[12] C. G. J. Jacobi, De usu legitimo formulae summatoriae Maclaurinianae, *J. Reine Angew Math.* **12** (1834), 263-272.

[13] D. E. Knuth, Johann Faulhaber and sums of powers, *Math. Comp.* **61** (203) (1993), 277-294.

[14] E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852), 93-146.

[15] G. Pietrocola, On polynomials for the calculation of sums of powers of successive integers and Bernoulli numbers deduced from the Pascal's triangle, www.pietrocola.edu

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

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

[18] Z-H. Sun, A note on Wilson's theorm and Wolstenholme's theorem, unpublished.

[19] C. von Staudt, Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend, *J. Reine Angew. Math.* **21** (1840), 372-374.