Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 74 (2019)
Heft: 4

Artikel: Another Wolstenholme-type congruence
Autor: Aebi, Christian
DOI: https://doi.org/10.5169/seals-869241

Elem. Math. 74 (2019) 169 – 175
0013-6018/19/040169-7
DOI 10.4171/EM/394

Elemente der Mathematik

Another Wolstenholme-type congruence

Christian Aebi

Christian Aebi, received his M.Sc. in 1990 from the University of Geneva, Switzerland. Ever since, he has been teaching there in both junior and senior high school, where he tries sharing as much as possible his passion for mathematics with his students.

1 Introduction

If in 1862 J. Wolstenholme [13] proved that *the numerator of the fraction* $1+\frac{1}{2}+\cdots+\frac{1}{n-1}$ *when reduced to its lowest terms* [*for a prime* $n>3$] *is divisible by* n^2, today one simply considers each term of the sum as the inverse of an element of $\mathbb{Z}_{n^2}$ and sets $\sum_{i=1}^{n-1}\frac{1}{i}\equiv 0 \pmod{n^2}$. The viewpoint has changed but the fascination remains intact. Combining the previous result with the fact that $\sum_{i=1}^{n-1}\frac{1}{i^2}\equiv 0 \pmod{n}$ allowed him to prove $\binom{2n-1}{n-1}\equiv 1 \pmod{n^3}$. At the dawn of the XX$^{\text{th}}$ century, J.W.L. Glaisher [3, 4] extended Wolstenholme's theorem, $\binom{2p-1}{p-1}\equiv 1 \pmod{p^3}$ to $\mathbb{Z}_{p^4}$ for primes $p>3$ and connected it to

Der sogenannte *erste Fall des Satzes von Fermat* besagt, dass $x^p+y^p\neq z^p$ für Primzahlen p mit $p\nmid xyz$ gilt. Bereits im Jahre 1847 realisierte Cauchy (siehe [12, p. 155]), dass $\sum_{i=1}^{(p-1)/2} i^{p-4}\equiv 0 \pmod{p}$ folgt, wenn dieser *erste Fall* für eine Primzahl p nicht gilt. Diese Summe wiederum ist über den kleinen Satz von Fermat verknüpft mit den Bernoulli-Zahlen und einem Resultat von Genocchi: $\sum_{i=1}^{(p-1)/2}\frac{1}{i^3}\equiv -2B_{p-3} \pmod{p}$. Derartige Summen wurden zu einer Quelle der Inspiration für Sylvester, Wolstenholme, Morley, Glaisher, Mirimanoff, Vandiver und Lehmer. In der vorliegenden Arbeit zeigt der Autor

$$\sum_{\substack{0<i<j<p\\ i \text{ odd},\, j \text{ even}}}\frac{1}{ij}\equiv -\frac{7}{48}pB_{p-3} \pmod{p^2}.$$

Eine Version dieser Summe modulo p war vor Kurzem die Grundlage für einen elementaren Beweis der Kongruenz von Morley.

Bernoulli numbers by obtaining $\binom{2p-1}{p-1} \equiv 1 - \frac{2}{3}p^3 B_{p-3} \pmod{p^4}$. More than half a century later, Selfridge and Pollack [10] identified the first irregular prime p dividing B_{p-3}. Another thirty years after, J. McIntosh [10] defined *Wolstenholme primes* as verifying one of the three equivalent conditions:

i) $\displaystyle\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$

ii) $p | B_{p-3}$

iii) $\displaystyle\sum_{1 \le k \le \lfloor \frac{p}{6} \rfloor + 1}^{\lfloor \frac{p}{4} \rfloor} \frac{1}{k^3} \equiv 0 \pmod{p}$

and thanks to the third condition confirmed the sole existence of two Wolstenholme primes smaller than $2 \cdot 10^8$. He also conjectured an infinite number of such primes for probabilistic reasons. Since then, no other Wolstenholme prime has been identified. A detailed account of the history of Wolstenholme-type congruences from the XIX$^{\text{th}}$ to the XXI$^{\text{th}}$ century is contained in [11].

Recently, an elementary proof of Morley's congruence theorem [1], $4^{p-1} \equiv \pm\binom{p-1}{\frac{p-1}{2}} \pmod{p^3}$, was found depending on the fact that

$$\sum_{\substack{0<i<j<p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} \equiv 0 \pmod{p} \quad \text{for primes } p > 3.$$

Our aim is to prove that

$$\sum_{\substack{0<i<j<p \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} \equiv -\frac{7}{48} p B_{p-3} \pmod{p^2}.$$

For example, in the case $p = 7$, one has

$$\begin{aligned} \frac{1}{1\cdot 2} + \frac{1}{1\cdot 4} + \frac{1}{1\cdot 6} + \frac{1}{3\cdot 4} + \frac{1}{3\cdot 6} + \frac{1}{5\cdot 6} &\equiv 25 + 37 + 41 + 45 + 30 + 18 \\ &= 196 \equiv 0 \pmod{7^2}. \end{aligned}$$

Our presentation relies almost exclusively on classical properties of Bernoulli numbers and polynomials from [8, Ch. 15] and [5] that we recall below.

2 Prerequisites

If we define in the standard way

$$S_m(p) := \sum_{i=1}^{p-1} i^m \tag{1}$$

then we have

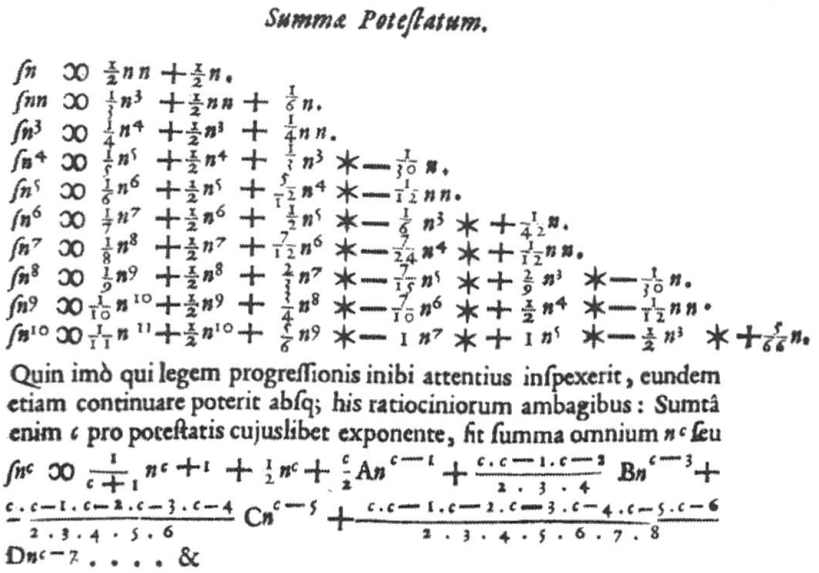
$$(m+1)S_m(p) = B_{m+1}(p) - B_{m+1} = \sum_{i=0}^{m+1} \binom{m+1}{i} p^{m+1-i} B_i, \tag{2}$$

where the B_m are the mth Bernoulli numbers given by

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} x^k,$$

and $B_m(x) := \sum_{k=0}^{m} \binom{m}{k} B_k x^{m-k}$ is the mth Bernoulli polynomial, which verifies the particular property

$$B_n\left(\frac{1}{2}\right) = (2^{1-n} - 1)B_n. \tag{3}$$


Summa Poteſtatum.

Quin imò qui legem progreſſionis inibi attentius inſpexerit, eundem etiam continuare poterit abſq; his ratiociniorum ambagibus: Sumtâ enim c pro poteſtatis cujuslibet exponente, fit ſumma omnium n^c ſeu

Figure 1 Jacob Bernoulli, *Ars Conjectandi*, 1713
With permission of Bibliotheque de Genève, Kc152, p. 97

3 Four progressive lemmas

We will start by recalling a very particular case of Leudesdorf's theorem [2, 5], that we prove for completeness.

Lemma 1. *If p is prime greater than 3, n is even and $p - 1 \nmid n$ then*

$$\sum_{1 \le i \le p-1} \frac{1}{i^n} \equiv \sum_{1 \le i \le \frac{p-1}{2}} \frac{1}{i^n} \equiv 0 \pmod{p}. \tag{4}$$

Proof. Let g denote a generator of $\mathbb{Z}_p^*$. Then

$$\sum_{1\leq i\leq p-1}\frac{1}{i^n}\equiv\sum_{1\leq i\leq p-1}\frac{1}{(gi)^n}\equiv\frac{1}{g^n}\sum_{1\leq i\leq p-1}\frac{1}{i^n}\equiv 0 \pmod p,$$

since $1/g^n \not\equiv 1 \pmod p$. If n is even then $i^n \equiv (p-i)^n \pmod p$ and so the second equivalence of (4) follows. □

Our second equivalence was already known to Genocchi in 1852 [12, p. 121] and generalized extensively in 2000 by Zhi-Hong Sun [14, Theorem 5.2.].

Lemma 2. *If p is prime and $p > 3$ then*

$$\sum_{0<i\leq\frac{p-1}{2}}\frac{1}{i^3}\equiv -2B_{p-3} \pmod p. \tag{5}$$

Proof. Working in $\mathbb{Z}_p$ we transform the summand in (5) into an expression of the form (1) by applying Fermat's little theorem, and follow up by the identities (2), (3) and (4):

$$\begin{aligned}\sum_{0<i\leq\frac{p-1}{2}}\frac{1}{i^3}&\equiv\sum_{0<i\leq\frac{p-1}{2}}i^{p-4}=S_{p-4}(\frac{p+1}{2})=\frac{1}{p-3}\left(B_{p-3}(\frac{p+1}{2})-B_{p-3}\right)\\&\equiv\frac{-1}{3}\left(B_{p-3}(\frac{1}{2})-B_{p-3}\right)\equiv\frac{-1}{3}\left((2^{4-p}-1)B_{p-3}-B_{p-3}\right)\equiv -2B_{p-3}.\end{aligned}$$ □

The next congruence is proposed as an exercise by Hao Pan in [7].

Lemma 3. *If p is prime and $p > 3$ then*

$$\sum_{\substack{0<i<j<p\\ j\text{ even}}}\frac{1}{i^2j}\equiv -\frac{3}{8}B_{p-3} \pmod p. \tag{6}$$

Proof. We proceed as above

$$\begin{aligned}\sum_{\substack{0<i<j<p\\ j\text{ even}}}\frac{1}{i^2j}&\equiv\sum_{\substack{0<i<j<p\\ j\text{ even}}}\frac{i^{p-3}}{j}=\sum_{\substack{0<j<p\\ j\text{ even}}}\frac{S_{p-3}(j)}{j}=\sum_{\substack{0<j<p\\ j\text{ even}}}\frac{B_{p-2}(j)-B_{p-2}}{j(p-2)}\\&\equiv-\sum_{\substack{0<j<p\\ j\text{ even}}}\frac{1}{2j}\sum_{k=0}^{p-2}\binom{p-2}{k}B_k j^{p-2-k}-B_{p-2}\\&\equiv-\frac{1}{2}\sum_{k=0}^{p-3}\sum_{\substack{0<j<p\\ j\text{ even}}}\binom{p-2}{k}B_k j^{p-3-k}\qquad\text{let } j=2m\end{aligned}$$

$$\equiv -\frac{1}{2}\sum_{k=0}^{p-3}\binom{p-2}{k}B_k\sum_{m=1}^{\frac{p-1}{2}}\frac{1}{(2m)^{k+2}}.$$

If $1 < k < p-3$ and k is odd then $B_k = 0$. Moreover if k is even, Leudesdorf's congruence (4) implies the last summand is 0. We are therefore left with the two terms $k = 1$ and $k = p-3$ to examine.

For $k = 1$ we get $-\frac{1}{2}(-2)\frac{-1}{2}\frac{1}{8}(-2B_{p-3}) = \frac{1}{8}B_{p-3}$ by using (5).

For $k = p-3$ we get $-\frac{1}{2}(-2)B_{p-3}\frac{-1}{2} = -\frac{1}{2}B_{p-3}$ by using Fermat.

Hence $\frac{1}{8}B_{p-3} + (-\frac{1}{2}B_{p-3}) = -\frac{3}{8}B_{p-3}$ gives the desired result. □

Our final lemma follows the same approach as the two preceding ones, but its proof requires all three conditions (3), (4) and (5).

Lemma 4. *If p is prime and $p > 3$ then*

$$\sum_{\substack{0<i<j<p\\ i \text{ and } j \text{ even}}}\frac{1}{i^2j} \equiv \frac{1}{16}B_{p-3} \pmod{p}.$$

Proof.

$$\sum_{\substack{0<i<j<p\\ i \text{ even, } j \text{ even}}}\frac{1}{i^2j} = \frac{1}{2^3}\sum_{0<m<n<\frac{p}{2}}\frac{1}{m^2n} \equiv \frac{1}{2^3}\sum_{0<m<n<\frac{p}{2}}\frac{m^{p-3}}{n}$$

$$= \frac{1}{2^3}\sum_{n=1}^{\frac{p+1}{2}}\frac{B_{p-2}(n) - B_{p-2}}{(p-2)n} = \frac{1}{2^3}\sum_{n=1}^{\frac{p+1}{2}}\frac{\sum_{k=0}^{p-2}\binom{p-2}{k}B_kn^{p-2-k} - B_{p-2}}{(p-2)n}$$

$$\equiv -\frac{1}{2^4}\sum_{n=1}^{\frac{p+1}{2}}\sum_{k=0}^{p-3}\binom{p-2}{k}B_kn^{p-3-k} \equiv -\frac{1}{2^4}\sum_{k=0}^{p-3}\binom{p-2}{k}B_k\sum_{n=1}^{\frac{p+1}{2}}\frac{1}{n^{k+2}}$$

$$\equiv -\frac{1}{2^4}\sum_{k=0}^{p-3}\binom{p-2}{k}B_k\left[\sum_{n=1}^{\frac{p-1}{2}}\frac{1}{n^{k+2}} + 2^{k+2}\right]$$

$$\equiv -\frac{1}{2^4}\sum_{k=0}^{p-3}\binom{p-2}{k}B_k\sum_{n=1}^{\frac{p-1}{2}}\frac{1}{n^{k+2}} - \frac{1}{2^2}\sum_{k=0}^{p-3}\binom{p-2}{k}B_k2^k.$$

In the first term we use the facts that $B_k = 0$ for all odd $k > 1$ and $\sum_{n=1}^{\frac{p-1}{2}}\frac{1}{n^{k+2}} \equiv 0 \pmod{p}$ when k is even and $k < p-3$, by (4). Hence we are left to examine the terms, $k = 1$ and $k = p-3$. By (5) we get

$$-\frac{1}{2^4}(-2)\frac{-1}{2}\cdot(-2B_{p-3}) + \frac{1}{2^3}B_{p-3}\cdot\frac{-1}{2} \equiv \frac{1}{16}B_{p-3} \pmod{p}.$$

Concerning the last term, we use (3):

$$\sum_{k=0}^{p-2} \binom{p-2}{k} B_k 2^k = 2^{p-2} B_{p-2}(\tfrac{1}{2}) = (2-2^{p-2})B_{p-2} = 0,$$

since $p-2$ is odd and $p > 3$. □

Theorem. *If p is prime and $p > 3$ then*

$$\sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{ij} \equiv -\frac{7}{48} p B_{p-3} \pmod{p^2}. \tag{7}$$

Proof. By exploiting three kinds of bijections as in [1], we see that

$$\begin{aligned}
3 \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{ij} &= \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{ij} + \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{(j-i)j} + \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{i(p+i-j)} \\
&= \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{p}{i(j-i)(p+i-j)} \cdot \frac{p-i+j}{p-i+j} \\
&\equiv p \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{p-i+j}{(-i)(j-i)(i-j)^2} \equiv p \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{(j-i)^2(-i)} \\
&\equiv p \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{i^2 j} \pmod{p^2},
\end{aligned}$$

where in the last passage we replaced $j-i$ by i and $p-i$ by j.

Therefore, combining the above with our two previous lemmas gives the final blow:

$$\begin{aligned}
\sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{ij} &\equiv \frac{p}{3} \sum_{\substack{0<i<j<p \\ i \text{ odd, } j \text{ even}}} \frac{1}{i^2 j} \equiv \frac{p}{3} \left(\sum_{\substack{0<i<j<p \\ j \text{ even}}} \frac{1}{i^2 j} - \sum_{\substack{0<i<j<p \\ i \text{ and } j \text{ even}}} \frac{1}{i^2 j} \right) \\
&\equiv \frac{p}{3} \left(-\frac{3}{8} B_{p-3} - \frac{1}{16} B_{p-3} \right) \equiv -\frac{7}{48} B_{p-3} \pmod{p^2}.
\end{aligned}$$

□

Acknowlegdment

The author thanks Grant Cairns, Gerhard Wanner and the referee for their constructive remarks and suggestions.

References

[1] Christian Aebi and Grant Cairns, *Morley's other miracle*, Math. Mag. 85 (2012), 205–211.

[2] ——, *Wolstenholme again*, Elemente der Mathematik, Volume 70, Issue 3, (2015), pp. 125–130.

[3] J.W.L. Glaisher, *Congruences relating to the sums of products of the first n numbers and to other sums of products*, Quart. J. Math. 31 (1900), 1–35.

[4] ——, *On the residues of the sums of products of the first* $p-1$ *numbers, and their powers, to modulus* p^2 *or* p^3, ibid., 321–353.

[5] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.

[6] Ernst Hairer, Gerhard Wanner, *Analysis by Its History*, Springer-Verlag, 2008.

[7] Hao Pan, *On a generalization of Carlitz's congruence*, https://arxiv.org/pdf/math/0603488.pdf.

[8] Keneth Ireland and Michael Rosen, *A classical introduction to number theory*, Springer-Verlag, 1998.

[9] C. Leudesdorf, *Some Results in the Elementary Theory of Numbers*, Proc. London Math. Soc. **S1-20** (1889), no. 1, 199–212.

[10] McIntosh Richard, *On the converse of Wolstenholme's theorem*, Acta Arithmetica **LXXI.4** (1995), 381–389.

[11] Romeo Meštrović, *Wolstenholme's theorem: Its generalizations and extensions in the last hundred and fifty years* (1862–2012), Preprint.

[12] Paulo Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[13] J. Wolstenholme, *On certain properties of prime numbers*, Q. J. Math. **5** (1862), 35–39.

[14] Zhi-Hong Sun, *Congruences concerning Bernoulli numbers and Bernoulli polynomials*, Discrete Applied Mathematics 1 **105** (2000), 193–223.

Christian Aebi
Collège Calvin
CH-1211 Geneva, Switzerland
e-mail: christian.aebi@edu.ge.ch