Elem. Math. 70 (2015) 125 – 130
0013-6018/15/030125-6
DOI 10.4171/EM/285

Elemente der Mathematik

Wolstenholme again

Christian Aebi and Grant Cairns

Christian Aebi studied mathematics in Geneva, Switzerland at the state university. He has been teaching there ever since, in both junior and senior high schools. He enjoys showing his students how an apparently elementary mathematical exercise, when slightly distorted, can sometimes lead to a non-trivial mathematical research problem.

Grant Cairns studied engineering and science at the University of Queensland, Australia, before doing doctoral studies under Pierre Molino in Montpellier, France. He benefited from two years in the stimulating environment of the University of Geneva. Since 1988 he has enjoyed teaching at La Trobe University in Melbourne Australia.

Thanks to Wolstenholme [14], the following three congruences have been known since 1862, for all primes $p \geq 5$:

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}, \tag{1}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}, \tag{2}$$

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p}. \tag{3}$$

Here of course, $\frac{1}{k}$ means the (multiplicative) inverse of k in the relevant sense: in $\mathbb{Z}_p$, $\mathbb{Z}_{p^2}$, etc, according to the context.

Die Partialsummen $s_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ der harmonischen Reihe wurden im Laufe der Zeit immer wieder untersucht. Wohlbekannt ist beispielsweise, dass s_n für kein $n > 1$ ganzzahlig ist. Für Primzahlen $p \geq 5$ fand Joseph Wolstenholme 1862, dass der Zähler von s_{p-1} durch p^2 teilbar ist. Verschiedene äquivalente Formulierungen und Folgerungen dieses Satzes sind bekannt. Falls nun s_{p-1} sogar durch p^3 teilbar ist, nennt man p eine Wolstenholme-Primzahl. Bislang wurden nur zwei derartige Primzahlen gefunden, aber man kennt von ihnen verschiedene äquivalente Charakterisierungen. Eine davon hat erstaunlicherweise mit den Bernoulli-Zahlen zu tun. Die Autoren des vorliegenden Artikels untersuchen diese seltenen Pflanzen im Primzahlgarten.

More than 125 years later, Gardiner [2] showed the relation between these equivalences when the degree is pushed one level higher:

Theorem 1. *If $p \geq 7$ is prime, the following conditions are equivalent:*

a) *p is a Wolstenholme prime, meaning :* $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$,

b) $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^3}$,

c) $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p^2}$,

d) *$p \mid B_{p-3}$ where B_k denotes the kth Bernoulli number.*

In 1988 the only known Wolstenholme prime was 16843. It had been identified while searching for irregular primes, which as Kummer had revealed are intimately connected to Fermat's last theorem [7]. In the same manner, the next Wolstenholme prime, 2124679, was discovered five years later by Buhler, Crandall, Ernvall and Metsänkylä [1]. The term *Wolstenholme prime* was introduced by McIntosh in his 1995 paper [12]. Ever since, no other Wolstenholme prime has been identified; see [10] for another equivalent condition. Nevertheless, Gardiner's result has been extended one degree further.

Theorem 2. *If $p \geq 7$ is prime, the following conditions are equivalent:*

a) $\binom{2p-1}{p-1} \equiv 1 \pmod{p^5}$,

b) $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^4}$,

c) $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p^3}$,

d) $p^2 \mid B_{p^3-p^2-2}$.

The above result is implicitly contained in Helou's and Terjanian's 2008 paper [5], but somewhat scattered amongst a raft of other, often more substantial results. We will say more on this at the end of this note. Our main goal here is to highlight the result itself, and to provide an elementary and direct proof. In so doing we hope this may also serve as an introduction to the more recent articles by experts in the field [12, 5, 9, 11, 13]. One basic classical result we use throughout this note is a particular case of Leudesdorf's theorem [8]; see also [4, Chap. VIII.8.7] and [3]. We provide a proof, for completeness.

Lemma. *If $p \geq 5$ is prime and $k \in \mathbb{N}$ then*

$$\sum_{1 \leq i \leq p-1} \frac{1}{i^k} \equiv \sum_{1 \leq i \leq \frac{p-1}{2}} \frac{1}{i^k} \equiv 0 \pmod{p}, \text{ if } k \text{ is even and } p-1 \nmid k, \tag{4}$$

$$\sum_{1 \leq i \leq p-1} \frac{1}{i^k} \equiv 0 \pmod{p^2}, \text{ if } k \text{ is odd and } p-1 \nmid k+1. \tag{5}$$

Proof. Consider a generator $a \in \mathbb{Z}_p^*$. Then

$$\sum_{1 \leq i \leq p-1} \frac{1}{i^k} \equiv \sum_{1 \leq i \leq p-1} \frac{1}{(ai)^k} \equiv \frac{1}{a^k} \sum_{1 \leq i \leq p-1} \frac{1}{i^k} \equiv 0 \pmod{p}$$

since $1/a^k \not\equiv 1 \pmod{p}$. When k is even, $1/i^k \equiv 1/(p-i)^k \pmod{p}$ and so (4) follows. When k is odd, notice that in $\mathbb{Z}_{p^2}$ we have:

$$\begin{aligned}\sum_{1\le i\le p-1}\frac{1}{i^k} = \sum_{1\le i\le (p-1)/2}\frac{1}{i^k}+\frac{1}{(p-i)^k} &\equiv \sum_{1\le i\le (p-1)/2}\frac{1}{i^k}+\frac{1}{kpi^{k-1}-i^k}\\ &\equiv kp\sum_{1\le i\le (p-1)/2}\frac{1}{kpi^k-i^{k+1}}\\ &\equiv -kp\sum_{1\le i\le (p-1)/2}\frac{1}{i^{k+1}}\equiv 0 \pmod{p^2},\end{aligned}$$

where the penultimate equivalence is obtained by amplification by the conjugate, $kpi^k + i^{k+1}$, and the last equivalence is by using (4). □

With that in hand we are set to provide the following:

Proof of Theorem 2. (a) ⇔ (c). We first develop the binomial coefficient $\binom{2p-1}{p-1}$ "downwards":

$$\begin{aligned}\binom{2p-1}{p-1} &= \frac{(2p-1)(2p-2)\cdots(2p-(p-1))}{1\cdot 2\cdots(p-1)}\\ &= (-1)^{p-1}\left(1-\frac{2p}{1}\right)\left(1-\frac{2p}{2}\right)\cdots\left(1-\frac{2p}{p-1}\right).\end{aligned}$$

Expanding the last line in $\mathbb{Z}_{p^5}$ gives us:

$$1-2p\sum_i\frac{1}{i}+4p^2\sum_{i<j}\frac{1}{ij}-8p^3\sum_{i<j<k}\frac{1}{ijk}+16p^4\sum_{i<j<k<l}\frac{1}{ijkl}, \tag{6}$$

where here and below, unless otherwise stated, the summations are over variables in the range $1,\ldots,p-1$.

Next we work "upwards":

$$\begin{aligned}\binom{2p-1}{p-1} &= \frac{(1+p)(2+p)\cdots((p-1)+p)}{1\cdot 2\cdots(p-1)}\\ &= \left(1+\frac{p}{1}\right)\left(1+\frac{p}{2}\right)\cdots\left(1+\frac{p}{p-1}\right)\end{aligned}$$

to obtain in $\mathbb{Z}_{p^5}$:

$$1+p\sum_i\frac{1}{i}+p^2\sum_{i<j}\frac{1}{ij}+p^3\sum_{i<j<k}\frac{1}{ijk}+p^4\sum_{i<j<k<l}\frac{1}{ijkl}. \tag{7}$$

Multiply equation (7) by 2 and add the product to equation (6) in order to eliminate the p term. Then divide both members by 3 to get:

$$\binom{2p-1}{p-1} \equiv 1 + 2p^2 \sum_{i<j} \frac{1}{ij} - 2p^3 \sum_{i<j<k} \frac{1}{ijk} + 6p^4 \sum_{i<j<k<l} \frac{1}{ijkl}. \tag{8}$$

Concerning the last summand, notice that multiplying all the indices i, j, k, l by 2 leaves the sum $\sum_{i<j<k<l} \frac{1}{ijkl}$ fixed in $\mathbb{Z}_p$. Therefore, since $2^4 \not\equiv 1 \pmod{p}$, this sum is equivalent to $0 \pmod{p}$.

The second summand may be transformed by using $2\sum \frac{1}{ij} = \left(\sum \frac{1}{i}\right)^2 - \sum \frac{1}{i^2}$. After substitution and application of (2) to the square term we get:

$$\binom{2p-1}{p-1} \equiv 1 - p^2 \sum_{i} \frac{1}{i^2} - 2p^3 \sum_{i<j<k} \frac{1}{ijk} \pmod{p^5}. \tag{9}$$

Finally, concerning the last summand, notice that we have:

$$6 \sum_{i<j<k} \frac{1}{ijk} = \left(\sum_i \frac{1}{i}\right)^3 - 3\left(\sum_i \frac{1}{i^2}\right)\left(\sum_j \frac{1}{j}\right) + 2\sum_i \frac{1}{i^3}, \tag{10}$$

which is equivalent to $0 \pmod{p^2}$ by using the equivalences (2), (3) and (5). Therefore we have proved

$$\binom{2p-1}{p-1} \equiv 1 - p^2 \sum_{i} \frac{1}{i^2} \pmod{p^5}, \tag{11}$$

which figures in [12, p. 385].

(b) $\Leftrightarrow$ (c). By using elementary identities we obtain:

$$\begin{aligned}
2\sum_i \frac{1}{i} &= \sum_i \left(\frac{1}{p-i} + \frac{1}{i}\right) = p \sum_i \left(\frac{1}{(p-i)i} + \frac{1}{i^2} - \frac{1}{i^2}\right) \\
&= -p \sum_i \frac{1}{i^2} + p^2 \sum_i \frac{1}{(p-i)i^2} \\
&= -p \sum_i \frac{1}{i^2} + p^2 \sum_i \left(\frac{1}{(p-i)i^2} + \frac{1}{i^3}\right) - p^2 \sum_i \frac{1}{i^3} \\
&= -p \sum_i \frac{1}{i^2} - p^2 \sum_i \frac{1}{i^3} + p^3 \sum_i \frac{1}{(p-i)i^3},
\end{aligned}$$

from which we easily conclude by using (5) on the middle summand and (4) on the last summand as $\sum_i \frac{1}{(p-i)i^3} \equiv \sum_i \frac{-1}{i^4} \pmod{p}$.

Equation (11) $\Leftrightarrow$ (d). This last equivalence requires basic knowledge of Bernoulli numbers we recall from [6]. If

$$S_m(p) := \sum_{i=1}^{p-1} i^m, \tag{12}$$

then from [6, p. 230, Theorem 1],

$$S_m(p) = \sum_{i=1}^{m+1} \frac{1}{i}\binom{m}{i-1} p^i B_{m+1-i}. \tag{13}$$

Importantly for us, the B_i are 0 for odd integers $i > 1$. Our general method is to transform the summand in (11) into an equation of the form (12) by applying Euler's theorem,

$$i^{-2} \equiv i^{\phi(p^3)-2} \pmod{p^3},$$

where ϕ is Euler's totient function. Working in $\mathbb{Z}_{p^3}$ and letting $m := p^3 - p^2 - 2$ we get

$$\sum_{i=1}^{p-1} i^{-2} \equiv \sum_{i=1}^{p-1} i^m = S_m(p) = \sum_{i=1}^{m+1} \frac{1}{i}\binom{m}{i-1} p^i B_{m+1-i}. \tag{14}$$

Since odd indexed Bernoulli numbers greater than one vanish, we apply a consequence of the von Staudt–Clausen theorem [6, p. 233, Theorem 3], which says that for n even

$$\operatorname{denom}(B_n) = \prod_{\substack{p-1 \mid n \\ p \text{ prime}}} p.$$

In particular, the denominator of B_n is square free; so it is at most divisible by p, and never by p^2. Furthermore, the denominators of B_{p-3} and B_{p-5} are not divisible by p, and since $p-1$ is not a divisor of $p^3 - p^2 - 2$ or $p^3 - p^2 - 4$, so p does not divide $B_{p^3-p^2-2}$ or $B_{p^3-p^2-2}$. As a consequence, all terms of the sum (14) vanish, except the first one, giving $pB_{p^3-p^2-2} \pmod{p^3}$, which replaced in (11) leads us to what is wanted:

$$\binom{2p-1}{p-1} \equiv 1 - p^3 B_{p^3-p^2-2} \pmod{p^5}. \qquad \square$$

An amusing aspect of the preceding theorem is that McIntosh commented that there is probably only a finite number of primes verifying criterion (a) of Theorem 2 and conjectured that there are none [12, bottom p. 387]. One natural question is: Can Theorem 2 be extended to the next degree? According to [5] it seems the answer is no, at least not just involving the divisibility of a single Bernoulli number. Indeed, Helou and Terjanian obtain the following results (see [5, Lemma 3 and Cor. 5(1)]):

$$\binom{2p-1}{p-1} \equiv 1 - p^3 B_{p^3-p^2-2} + \frac{1}{3}p^5 B_{p-3} - \frac{6}{5}p^5 B_{p-5} \pmod{p^6},$$

$$\sum_{i=1}^{p-1} \frac{1}{i} \equiv -\frac{p^2}{2} B_{p^3-p^2-2} + \frac{p^4}{6} B_{p-3} - \frac{p^4}{5} B_{p-5} \pmod{p^5},$$

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv p B_{p^3-p^2-2} - \frac{p^3}{3} B_{p-3} + \frac{4}{5} p^3 B_{p-5} \pmod{p^4},$$

and so the last term in B_{p-5} does not coincide in any pair of expressions. Notice that reducing these three equivalences modulo p^5, p^4, p^3 respectively establishes Theorem 2. It is in this sense that Theorem 2 is contained in [5]. A formula for $\binom{2p-1}{p-1}$ modulo p^7 is given in [11].

References

[1] J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä, *Irregular primes and cyclotomic invariants to four million*, Math. Comp. **61** (1993), 151–153.

[2] A. Gardiner, *Four problems on prime power divisibility*, Amer. Math. Monthly **95** (1988), no. 10, 926–931.

[3] Ira Gessel, *Wolstenholme Revisited*, Amer. Math. Monthly **105** (1998), 657–658.

[4] 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.

[5] Charles Helou and Guy Terjanian, *On Wolstenholme's theorem and its converse*, J. Number Theory **128** (2008), no. 3, 475–499.

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

[7] Emma Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. (2) **39** (1938), no. 2, 350–360.

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

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

[10] ———, *On a congruence modulo n^3 involving two consecutive sums of powers*, J. Integer Seq. **17** (2014), no. 8, Article 14.8.4, 20.

[11] ———, *On the* mod p^7 *determination of* $\binom{2p-1}{p-1}$, Rocky Mountain J. Math. **44** (2014), no. 2, 633–648.

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

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

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

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

Grant Cairns
La Trobe University
Melbourne, Australia 3086
e-mail: G.Cairns@latrobe.edu.au