Elemente der Mathematik 78 (2023), 35–36
DOI 10.4171/EM/457

Short note Wolstenholme's theorem revisited

Arpan Kanrar

Abstract. We give an elementary proof that for primes $p > 3$ the numerator of the reduced fraction $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ is divisible by p^2.

In 1862, J. Wolstenholme [5] proved that, for all primes $p > 3$, the numerator of the reduced fraction of the harmonic sum

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is divisible by p^2. In this note, we present an elementary proof based essentially on Fermat's little theorem and Lagrange's theorem relating the number of roots of a polynomial to its degree. Other proofs may be found in [3, p. 116], [2, p. 89] or [1, Lemma].

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

$$p^2 \mid (p-1)!\Big(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}\Big).$$

Proof. One easily sees that the above integer is divisible by p by using symmetry:

$$(p-1)!\sum_{i=1}^{p-1}\frac{1}{i} = (p-1)!\sum_{i=1}^{\frac{p-1}{2}}\Big(\frac{1}{p-i} + \frac{1}{i}\Big) = p\sum_{i=1}^{\frac{p-1}{2}}\frac{(p-1)!}{i(p-i)}.$$

Hence, let

$$a_i := \frac{(p-1)!}{i(p-i)} \quad \text{and} \quad A := \sum_{i=1}^{\frac{p-1}{2}} a_i,$$

that we are to prove A is divisible by p. For that matter, we define

$$f(x) := \prod_{i=1}^{\frac{p-1}{2}}(x - a_i) - (x^{\frac{p-1}{2}} - 1).$$

Notice first that the a_i are all distinct since, if $1 \le i < j < \frac{p-1}{2}$ and $a_i \equiv a_j$, then

$$0 \equiv j^2 - i^2 \equiv (j-i)(j+i) \pmod p$$

gives a contradiction. Second, we have

$$a_i = \left(\frac{p-1}{2}\right)! \, \frac{1}{i}\left(p - \frac{p-1}{2}\right) \cdots (p-2)(p-1)\frac{1}{p-i} \equiv (-1)^{\frac{p+1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \frac{1}{i^2}.$$

Thus, by Fermat's little theorem, $a_i^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ since $8 \mid (p^2-1)$ for odd numbers. Hence, $f(a_i) \equiv 0 \pmod{p}$ for all $\frac{p-1}{2}$ values. Finally, notice that the leading coefficient of f is A, and its degree in $\mathbb{Z}[x]$ is $\frac{p-3}{2}$. Consequently, by Lagrange's theorem [2, Theorem 5.21], we deduce that $p \mid A$. ■

Remark. The same method of proof allows one to obtain Wilson's theorem from Fermat's theorem by considering the polynomial $g(x) := \prod_{i=1}^{p-1}(x-i) - (x^{p-1}-1)$. We recommend [4] for an even more elementary proof of both results above.

Acknowledgements. The author is grateful to the referee for going through the earlier draft meticulously and suggesting a nice way for a neat proof. The author is thankful to Professor R. Thangadurai for his guidance throughout the preparation of this manuscript.

Funding. I would like to acknowledge the Department of Atomic Energy, Govt. of India for providing the research grant.

References

[1] C. Aebi and G. Cairns, Wolstenholme again. *Elem. Math.* **70** (2015), no. 3, 125–130.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*. Springer-Verlag, New York, 2000.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Fifth edn., The Clarendon Press, Oxford University Press, New York, 1979.

[4] S. Hussein, *Wilson's and Wolstenholme's theorems*, preprint, https://arxiv.org/pdf/1809.04767.pdf.

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

Arpan Kanrar
Harish-Chandra Research Institute, HBNI
Chhatnag Road, Jhunsi, Prayagraj – 211019, India
arpankanrar@hri.res.in