Wolstenholme Revisited

Ira M. Gessel

A recently Monthly article [1, Theorem 4] gave an incorrect proof of the following result (which was also stated incorrectly): Let p be a prime and let k be a nonnegative integer such that $k < p-2$. Then the numerator of the fraction

$$\sum_{\substack{1\le i<p^n\\(i,p)=1}} \frac{1}{i^k}$$

is divisible by p^n if k is even and by p^{n+1} if k is odd.

It is not difficult to give an elementary proof of a much stronger result. Let m and k be positive integers, and let

$$S(m,k) = \sum_{i\in R_m} \frac{1}{i^k},$$

where R_m is the set of integers from 1 to $m-1$ relatively prime to m. We first prove two lemmas about the numbers $S(m,k)$. It is convenient to use the notation $u \equiv v \pmod m$, where u and v are rational numbers, to mean that $u-v$ is a rational number whose numerator, in lowest terms, is divisible by m.

Lemma 1. *If a is an integer relatively prime to m then $(a^k-1)S(m,k) \equiv 0 \pmod m$.*

Proof. The set $\{\, ai \mid i \in R_m \,\}$, reduced modulo m, is R_m. It follows that

$$S(m,k) \equiv \sum_{i\in R_m} \frac{1}{(ai)^k} = \frac{1}{a^k} S(m,k) \pmod m. \quad \blacksquare$$

Lemma 2. *If k is odd then $2S(m,k) \equiv -mkS(m,k+1) \pmod{m^2}$.*

Proof. We have

$$2S(m,k) = \sum_{i\in R_m} \left(\frac{1}{i^k} + \frac{1}{(m-i)^k}\right) = \sum_{i\in R_m} \frac{i^k + (m-i)^k}{i^k(m-i)^k}.$$

Since k is odd, the binomial theorem yields $i^k + (m-i)^k \equiv ki^{k-1}m \pmod{m^2}$, and $(m-i)^k \equiv -i^k \pmod m$. Thus

$$2S(m,i) \equiv \sum_{i\in R_m} \frac{ki^{k-1}m}{i^k(-i^k)} \equiv -km \sum_{i\in R_m} \frac{1}{i^{k+1}} \pmod{m^2}. \quad \blacksquare$$

It can be shown, by similar reasoning, that the congruence of Lemma 2 actually holds modulo m^3.

The following results generalize those of [1].

Theorem 1. *If k is not a multiple of $p-1$ for any prime p dividing m, then $S(m,k) \equiv 0 \pmod m$.*

Proof. The hypothesis implies that for each prime p dividing m, we can find an integer a_p such that $a_p^k - 1$ is not divisible by p. Now let a be congruent to a_p modulo p for each p and apply Lemma 1. $\blacksquare$

The next result follows immediately from Theorem 1 and Lemma 2:

Theorem 2. *If k is odd, and $k+1$ is not a multiple of $p-1$ for any prime p dividing m, then $S(m,k) \equiv 0 \pmod{m^2}$.* $\blacksquare$

Similar results can be found for those cases not covered by Theorems 1 and 2. For example, $S(2^j,k) \equiv 0 \pmod{2^{j-1}}$, and for k odd, $S(2^j,k) \equiv 0 \pmod{2^{2(j-1)}}$.

References

1. M. Bayat, A generalization of Wolstenholme's theorem, *Amer. Math. Monthly* 104 (1997) 557–560.

Department of Mathematics
Brandeis University
Waltham, MA 02254-9110
gessel@math.brandeis.edu

Note. *This version corrects two minor errors in the first paragraph of the published version.*