Canad. Math. Bull. Vol. **33** (2), 1990

A (MODEST) GENERALIZATION OF THE THEOREMS OF WILSON AND FERMAT

BY

W. O. J. MOSER

ABSTRACT. We show that $(1/n^2)\sum_{d|n} a^d(\varphi(n/d))^2(n/d)^d d!$ is an integer. Special cases include the theorems of Wilson and Fermat.

The classical congruence of Wilson states that

$$(1) \qquad (p-1)!+1 \equiv 0 \pmod p, \quad p \text{ a prime,}$$

while Fermat's congruence states that

$$(2) \qquad a^p \equiv a \pmod p, \quad p \text{ a prime.}$$

Traditionally these congruences are proved separately (and similarly), but L. Moser [2] observed that the same sort of proof yields, at once, the congruence

$$(3) \qquad a^p(p-1)! \equiv a(p-1) \pmod p, \quad p \text{ a prime.}$$

Taking $a = 1$ in (3) gives (1), and then (1) and (3) give (2).

In this note we prove that for integers $a \geqq 1$ and $n \geqq 2$

$$(4) \qquad \frac{1}{n^2}\sum_{d|n} a^d\left(\varphi\left(\frac{n}{d}\right)\right)^2\left(\frac{n}{d}\right)^d d! \text{ is an integer.}$$

Here $\varphi(n)$, the Euler phi function, denotes the number of integers in $\{1, 2, \ldots, n-1\}$ relatively prime to n, and we will be using $d \mid n$ to denote "d divides n" and (m, n) to denote the greatest common divisor of m and n. When $n = p$, a prime, (4) reads

$$\frac{1}{p^2}\{a(p-1)^2p + a^p p!\} \quad \text{is an integer,}$$

from which (3) follows, so (4) is indeed a (modest) generalization of (3).

First we will prove (4) in the case $a = 1$.

Consider the set S_n of $n!$ permutations (linear arrangements)

$$\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n), \quad \alpha_i \in \{1, 2, \ldots, n\}, \quad \alpha_i \neq \alpha_j \text{ if } i \neq j.$$

Received by the editors January 9, 1989.

AMS (1980) Subject Classification: 11A07, 05A15.

https://doi.org/10.4153/CMB-1990-040-6 Published online by Cambridge University Press

Let T denote the operation

$$T(\underline{\alpha}) = T(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha_2, \alpha_3, \ldots, \alpha_n, \alpha_1),$$

and R the operation

$$R(\underline{\alpha}) = R(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha_1 + 1, \alpha_2 + 1, \ldots, \alpha_n + 1), \quad n + 1 = 1.$$

It is easy to see that T and R commute i.e., $T(R(\underline{\alpha})) = R(T(\underline{\alpha}))$ for all $\underline{\alpha} \in \mathcal{S}_n$, that T and R each generate a cyclic group of order n, and that T and R together generate a group $\mathcal{G}$ of order n^2 (the direct product of the two cyclic groups) whose elements are $T^{-m}R^k(1 \leqq m, k \leqq n)$. This group acts on $\mathcal{S}_n$, and partitions the set $\mathcal{S}_n$ into equivalence classes, where $\underline{\alpha}$ and $\underline{\beta}$ in $\mathcal{S}_n$ are equivalent if, for some m and k, $T^{-m}R^k(\underline{\alpha}) = \underline{\beta}$ or $R^k(\underline{\alpha}) = T^m(\underline{\beta})$.

Let $f(n)$ denote the number of these equivalence classes. J. E. Steggall [3] gave a method for computing $f(n)$ which involved setting up and solving a system of equations, but he failed to obtain the very simple expression

$$f(n) = \frac{1}{n^2} \sum_{d|n} \left(\varphi\left(\frac{n}{d}\right)\right)^2 \left(\frac{n}{d}\right)^d d!.$$

We will obtain this formula by applying Burnside's Lemma (see [2]), which states that

(5) $$f(n) = \frac{1}{n^2} \sum_{1 \leqq m,k \leqq n} \mathcal{N}(m,k), \quad \text{where } \mathcal{N}(m,k) = \#\{\underline{\alpha} \in \mathcal{S}_n \mid R^k(\underline{\alpha}) = T^m(\underline{\alpha})\}.$$

Note that:

(6) $$\begin{aligned} R^{ik}(\underline{\alpha}) &= (R^k)^i(\underline{\alpha}) = (R^k)^i(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\beta_1, \beta_2, \ldots, \beta_n), \\ \beta_s &= \alpha_s + ik; \text{ (the entries } \alpha_s + ik \text{ are, of course, reduced} \\ &\qquad (\text{mod } n) \text{ to be in the set } \{1, 2, \ldots, n\}); \end{aligned}$$

(7) $$\begin{aligned} T^{jm}(\underline{\alpha}) &= (T^m)^j(\underline{\alpha}) = (T^m)^j(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\beta_1, \beta_2, \ldots, \beta_n), \\ \beta_s &= \alpha_{s+jm}; \text{ (the subscripts } s + jm \text{ are, of course, reduced} \\ &\qquad (\text{mod } n) \text{ to be in the set } \{1, 2, \ldots, n\}); \end{aligned}$$

(8) $$\text{the period of } R^k \text{ in } \mathcal{G} \text{ is } \frac{n}{(n,k)};$$

(9) $$\text{the period of } T^m \text{ in } \mathcal{G} \text{ is } \frac{n}{(n,m)};$$

https://doi.org/10.4153/CMB-1990-040-6 Published online by Cambridge University Press

(10) $$\text{if } R^k(\underline{\alpha}) = T^m(\underline{\alpha}) \text{ for some } \underline{\alpha} \in \mathcal{S}_n \text{ then } (n,k) = (n,m).$$

The last assertion can be seen as follows. The first entry of $R^{kn/(n,k)}(\underline{\alpha})$ is α_1 (this follows from (6) and (8)), while the first entry of $T^{mn/(n,k)}(\underline{\alpha})$ is $\alpha_{1+mn/(n,k)}$ (this follows from (7)). Thus, if $R^k(\underline{\alpha}) = T^m(\underline{\alpha})$ then $\alpha_1 = \alpha_{1+mn/(n,k)}$, implying $mn/(n,k)$ is a multiple of n, so that $(n,k) \mid m$. Since $(n,k) \mid n$ it follows that $(n,k) \mid (n,m)$. Similarly $(n,m) \mid (n,k)$.

Using (10), (5) becomes

(11) $$f(n) = \frac{1}{n^2} \sum_{\substack{(m,n)=(k,n) \\ 1 \leqq m,k \leqq n}} \mathcal{N}(m,k) = \frac{1}{n^2} \sum_{d \mid n} \sum_{\substack{(m,n)=d \\ (k,n)=d}} \mathcal{N}(m,k).$$

Now for given d, m and k with $d \mid n$ and $(m,n) = (k,n) = d$ let us determine $\mathcal{N}(m,k)$. Suppose that $\underline{\alpha} \in \mathcal{S}_n$ and

(12) $$R^k(\underline{\alpha}) = T^m(\underline{\alpha}).$$

Then
$$T^{im}(\underline{\alpha}) = R^{ik}(\underline{\alpha}), \quad i = 1, 2, \ldots, \frac{n}{d}$$
and hence
$$\alpha_{s+im} = \alpha_s + ik, \quad i = 1, 2, \ldots, \frac{n}{d}; \quad s = 1, 2, \ldots, d.$$
Thus the entries $\alpha_1, \alpha_2, \ldots, \alpha_d$ determine all other entries in $(\alpha_1, \alpha_2, \ldots, \alpha_n)$,
$$\alpha_1, \alpha_2, \ldots, \alpha_d \text{ are pairwise incongruent } \pmod{k}$$
(because R^k has period n/d), and $(\alpha_1, \alpha_2, \ldots, \alpha_d)$ must be a permutation of $(\beta_1, \beta_2, \ldots, \beta_d)$, where
$$\beta_1 \in \left\{1, 1+k, 1+2k, \ldots, 1 + \left(\frac{n}{d} - 1\right)k\right\}$$
$$\beta_2 \in \left\{2, 2+k, 2+2k, \ldots, 2 + \left(\frac{n}{d} - 1\right)k\right\}$$
$$\vdots$$
$$\beta_d \in \left\{d, d+k, d+2k, \ldots, d + \left(\frac{n}{d} - 1\right)k\right\}$$
Since there are n/d choices for each β_i, and each permutation of $(\beta_1, \beta_2, \ldots, \beta_d)$ leads to $d!$ permutations $(\alpha_1, \alpha_2, \ldots, \alpha_d)$ there are $(n/d)^d d!$ permutations $\underline{\alpha}$ satisfying (12):
$$\mathcal{N}(m,k) = \left(\frac{n}{d}\right)^d d! \quad \text{if} \quad (m,n) = (k,n) = d \quad \text{and} \quad d \mid n.$$

Now we have

$$f(n) = \frac{1}{n^2} \sum_{d|n} \sum_{\substack{(m,n)=d \\ (k,n)=d}} \left(\frac{n}{d}\right)^d d! \tag{13}$$
$$= \frac{1}{n^2} \sum_{d|n} \left(\frac{n}{d}\right)^d d! \sum_{(k,n)=d} \sum_{(m,n)=d} 1$$
$$= \frac{1}{n^2} \sum_{d|n} \left(\frac{n}{d}\right)^d d! \left(\varphi\left(\frac{n}{d}\right)\right)^2.$$

Of course $f(n)$ is an integer so we have (4) when $a = 1$.

When $a \geqq 2$, (4) is obtained by applying Burnside's Lemma to the set $\mathcal{S}_n \times \mathcal{C}_n$, where

$$\mathcal{C}_n = \{(c_1, c_2, \ldots, c_n) \mid c_1, c_2, \ldots, c_n \in \{1, 2, \ldots, n\}\}$$

and the group acting on $\mathcal{S}_n \times \mathcal{C}_n$ is generated by the two operations

$T : (\underline{\alpha}, \underline{c}) \longrightarrow (T(\underline{\alpha}), T(\underline{c}))$, where $T(\underline{c}) = T(c_1, c_2, \ldots, c_n) = (c_2, \ldots, c_n, c_1)$,

$R : (\underline{\alpha}, \underline{c}) \longrightarrow (R(\underline{\alpha}), \underline{c})$.

REFERENCES

1. C. L. Liu, *Introduction to Combinatorial Mathemamatics*, McGraw Hill, New York, 1968.

2. L. Moser, *On the theorems of Wilson and Fermat*, Scripta Mathematica, **22** (1956), 288.

3. J. E. Steggall, *On the number of patterns which can be derived from certain elements*. Messenger of Mathematics, **32** (1907), 56–61.

Department of Mathematics and Statistics
McGill University
905 Sherbrooke St. W.
Montreal, Que.
Canada H3A2K6