CONGRUENCE RELATIONS BETWEEN THE TRACES OF MATRIX POWERS

J. S. FRAME

1. Introduction. Let A be a matrix of finite order n and finite degree d, whose characteristic roots are certain n^{th} roots of unity $\alpha_1, \alpha_2, \ldots, \alpha_d$. We wish to prove a congruence (6) between the traces (tr) of certain powers of A, which is suggested by two somewhat simpler congruences (1) and (3).

First, if tr (A) is a rational integer, it is easy to establish the familiar congruence

$$\text{tr}(A) \equiv \text{tr}(A^p) \pmod{p},\ p \text{ prime}, \tag{1}$$

even though $\text{tr}(A^p)$ may not itself be rational. For we have

$$[\text{tr}(A)]^p = \left[\sum_{\nu=1}^{d} \alpha_\nu\right]^p = \sum_{\nu=1}^{d} \alpha_\nu^p + p(\ldots) = \text{tr}(A^p) + p(\ldots) \tag{2}$$

where $(\ldots)$ denotes an algebraic integer. The left-hand members of (1) and (2) are rational integers which are congruent (mod p) by Fermat's theorem. The right-hand members are explicitly congruent (mod p). Hence (1) follows from (2).

Secondly, for any integer a, we have

$$a^{p^\beta} \equiv a^{p^{\beta-1}} \pmod{p^\beta}, \text{ if } p^\beta \text{ is a prime power} > 1. \tag{3}$$

Equation (3) is trivial if a is divisible by p. Otherwise it can be established easily by setting $m = p^\beta$ in the well-known Euler congruence

$$a^{\phi(m)} \equiv 1 \pmod{m}, \qquad \text{for } (a, m) = 1, \tag{4}$$

where $\phi(m)$ is the Euler ϕ-function, and $\phi(p^\beta) = p^\beta - p^{\beta-1}$.

It is our purpose to prove a congruence relation (mod p^β), which generalizes (1) and is similar to (3), between the traces of certain powers of a matrix A of finite order—or, in other words, between certain sums of powers of roots of unity.

THEOREM. *Let $S(m)$ denote the trace of the m^{th} power of a matrix A of finite order n and finite degree $S(0)$, and assume that A is such that*

$$S(k) = S(1), \textit{ for all } k \textit{ such that } (k, n) = 1. \tag{5}$$

Then

$$S(p^\beta) \equiv S(p^{\beta-1}) \pmod{p^\beta}. \tag{6}$$

We note that condition (5) implies that A has a rational integral trace, but that not every matrix with rational integral trace satisfies (5).

Received July 21, 1948.

2. Proof of the theorem.[1] Let us define a "p^β-set" to be a set of roots of unity such that the sum of its p^{β}th powers are congruent to the sum of its $p^{\beta-1}$th powers mod p^β as in (6). We note that the negative of any root of unity is also a root of unity.

LEMMA 1. *The set of all the n distinct n^{th} roots of unity is a p^β-set.*

Proof. Denoting the sum of m^{th} powers by $S_n(m)$ we have

$$S_n(p^\beta) = n, \text{ if } n \text{ divides } p^\beta, \tag{7}$$
$$= 0, \text{ if } n \text{ does not divide } p^\beta.$$

Hence

$$S_n(p^\beta) - S_n(p^{\beta-1}) = p^\beta \text{ if } n = p^\beta, \tag{8}$$
$$= 0 \text{ otherwise.}$$

LEMMA 2. If one p^β-set is included as a subset of a larger p^β-set, the difference of the two p^β-sets is also a p^β-set. Furthermore, any set of roots of unity which is made up of two or more p^β-sets is also a p^β-set.

Proof. If each of two or more quantities $S(p^\beta) - S(p^{\beta-1})$ is congruent to 0, so is their sum or difference.

LEMMA 3. The set of $\phi(n)$ primitive n^{th} roots of unity is a p^β-set.

For prime n the lemma is a special case of Lemma 2. Assuming as induction hypothesis that the lemma is true for all ν with a smaller number of prime factors than n, we show that it is also true for n by applying Lemmas 1 and 2, and eliminating from the complete set of n n^{th} roots all sets of primitive ν^{th} roots for each ν which is a proper divisor of n. Only the primitive n^{th} roots remain. They form a p^β-set.

We observe that condition (5) implies that for any factor μ of n the primitive μ^{th} roots occur as roots of the matrix A with equal multiplicity. Hence by Lemmas 2 and 3 the roots of A are a p^β-set, so the theorem is established.

3. Applications of the theorem. In constructing the table of characters for a finite group, our theorem may be applied to determine many of the entries. For example, the symmetric group of degree 5 and order 120 has irreducible representations of degrees 1, 1, 4, 4, 5, 5, 6. There are 15 conjugate elements of order 2 which are squares of elements of order 4. Hence their traces form a vector of unitary squared length 120/15 which is unitary orthogonal to the vector (1, 1, 4, 4, 5, 5, 6) and congruent to it (mod 4). The only integral solution is (1, 1, 0, 0, 1, 1, −2). Similarly for the traces of the 24 elements of order 5 we have the vector (1, 1, −1, −1, 0, 0, 1) as is known by the ordinary modular theory (mod 5). Given the numbers of elements in the classes of conjugates, the table is completely determined by these congruences.

Michigan State College

[1] I am indebted to Professor R. Brauer for some suggestions for shortening my original proof.