HADAMARD'S DETERMINANT THEOREM AND THE SUM OF FOUR SQUARES

BY JOHN WILLIAMSON

We shall call a square matrix of order n an Hadamard matrix [1; 243] or, for brevity, an H-matrix, if all elements of the matrix are plus one or minus one and if its determinant has the maximum possible value $n^{\frac{1}{2}n}$. If A is an H-matrix and A' is the transpose of A, it is known that $AA' = nE_n$, where E_n is the unit matrix of order n. For an H-matrix of order $n > 1$ to exist n must have the value two or be congruent to zero modulo four [2; 311]. Whether or not an H-matrix of order n exists for any n congruent to zero modulo four is as yet undetermined. It is known however that an H-matrix of order n does exist when (i) $n = 2$ [2; 312]; (ii) $n = p^h + 1 \equiv 0 \pmod 4$, p an odd prime [2; 314]; (iii) $n = 2(p^h + 1)$, p an odd prime [2; 315]; (iv) $n = p(p + 1)$, p an odd prime $\equiv 3 \pmod 4$ [3; 1443]. Since the direct product of two H-matrices is an H-matrix [2; 312], an H-matrix does exist of any order which is a product of factors of types (i), (ii), (iii) or (iv).

In the first part of this paper we show that for (iii) we may substitute $n = m(p^h + 1)$, where $m > 1$ is the order of an H-matrix and p is an odd prime and for (iv) $n = N(N - 1)$, where N is a product of any number of factors of types (i) or (ii).

In the second part we investigate a seeming connection between special H-matrices of order $4n$, the n-th roots of unity and the representation of $4n$ as the sum of the squares of four integers. A very interesting theorem in this connection is proved for specific small values of n and from this theorem, when $n = 43$, the existence of an H-matrix of order 172 is deduced—the number 172 is not a product of factors of types (i), (ii), (iii) or (iv).

1. We first prove the following lemma.

LEMMA 1. *Let S be a square matrix of order n such that $S = \epsilon S'$, $\epsilon = \pm 1$, and such that $SS' = (n - 1)E_n$. Further, let A and B be two square matrices of order m satisfying the matric equations $AA' = BB' = mE_m$ and $AB' = -\epsilon BA'$. Then the matrix $K = A \cdot E_n + B \cdot S$, where $A \cdot E_n$ and $B \cdot S$ are the direct products of the matrices A, E_n and B, S respectively, satisfies the equation $KK' = mnE_{mn}$.*

Proof.

$$\begin{aligned} KK' &= (A \cdot E_n + B \cdot S)(A' \cdot E_n + B' \cdot S') \\ &= AA' \cdot E_n + BA' \cdot S + AB' \cdot S' + BB' \cdot SS' \\ &= mE_m \cdot E_n + BA' \cdot S - \epsilon BA' \cdot \epsilon S + mE_m \cdot (n-1)E_n \\ &= mE_m \cdot E_n + m(n-1)E_m \cdot E_n = mnE_{mn}. \end{aligned}$$

Received August 6, 1943; in revised form December 1, 1943.