AN ESTIMATE FOR THE ORDER OF RATIONAL MATRICES

Randee Putz

In this note we prove what we believe to be a new result concerning matrices, namely, that if an $n \times n$ matrix with rational entries has a finite order then this order is bounded. We also give an estimate for this bound and an application.

First we prove a number theoretic lemma which we shall use for our estimate.

LEMMA. Let $\pi(n)$ denote the number of primes less than n. Also let $C(n) = \Pi(p/p-1)$ where the product is taken over the first $\pi(n)$ primes. Let $m_1, \ldots, m_n$ be integers for which $\phi(m_j) \leq n$ $(j = 1, \ldots, n)$ (where ϕ denotes Euler's function) and $m = [m_1, \ldots, m_n]$ their least common multiple. Then

$$m \leq C(n+1)\, n^{\pi(n+1)} .$$

<u>Proof.</u> Let $m = p_1^{r_1} \ldots p_s^{r_s}$ be the prime decomposition of m. The fact that m is the least common multiple of $m_1, \ldots, m_n$ implies that $p_i^{r_i}$ must appear as a factor of some m_j. Furthermore, since by hypothesis $\phi(m_j) \leq n$, we have $\phi(p_i^{r_i}) \leq n$, that is, $p_i^{r_i} \leq n(p_i/p_i - 1)$. Moreover, as a factor of $\phi(p_i^{r_i})$, also $p_i - 1 \leq n$ and hence $p_i \leq n+1$. Therefore, as $s \leq \pi(n+1)$,

$$m = \prod_{i=1}^{s} p_i^{r_i} \leq C(n+1)\, n^{\pi(n+1)} .$$

THEOREM. Let A be an $n \times n$ rational matrix. If A

https://doi.org/10.4153/CMB-1967-044-x Published online by Cambridge University Press

has order m then

$$m \leq e^C (\log(n+1))(1+1/\log^2(n+1))\, n^{\pi(n+1)} ,$$

where C is Euler's constant.

Proof. Let $c_1, \ldots, c_n$ denote the eigenvalues of A. The fact that $A^m = I$ implies that A is diagonizable (3, p.343) and therefore, there exists a basis in complex n space of corresponding characteristic vectors $x_1, \ldots, x_n$. From the fact that $A x_i = c_i x_i$ we have $A^k x_i = c_i^k x_i$, and therefore that the eigenvalues of A are roots of unity. (This shows that a necessary condition for A to have finite order is that the coefficients of its characteristic polynomial must be dominated in absolute value by the coefficients of the polynomial $(z+1)^n$.) Suppose that c_i is a primitive m_i-th root of unity, and let r denote the least common multiple of $m_1, \ldots, m_n$. Because $x_1, \ldots, x_n$ form a basis and $c_i^r = 1$, we have $A^r = I$. But r is less than or equal to the order m, so $r = m$. Thus m is the least common multiple of $m_1, \ldots, m_n$.

Now the minimal polynomial of c_i over the rationals has degree $\phi(m_i)$ (4, p.160). Therefore, since the characteristic polynomial of A has rational coefficients and is of degree n, we have $\phi(m_i) \leq n$. Thus by the lemma, $m \leq C(n+1)\, n^{\pi(n+1)}$. From (2) we have the following estimate for $C(n+1)$, $C(n+1) \leq e^C (\log(n+1))(1+1/\log^2(n+1))$ (which yields the theorem), and an approximate value for e^C, $e^C = 1.78107\ 24179\ 90198$.

REMARK. For a particular n one can compute for each i the greatest exponent r_i occurring in the prime decomposition of m, and denote it by s_i. The estimate for m then becomes $m \leq p_1^{s_1} \cdots p_{\pi(n+1)}^{s_{\pi(n+1)}} = N$, whence we see that at most $(s_1+1) \ldots (s_{\pi(n+1)}+1)$ of the numbers less than or equal to N are possibilities for the order of a given $n \times n$ rational matrix. For example if $n = 5$ the proof of the theorem shows that $m \leq 2^3 \cdot 3 \cdot 5 = N$, (whereas using $C(6) \cdot 5^3$ as an estimate only yields $m \leq 468$) and that only sixteen numbers less than or equal to 120 are possibilities for the order of a rational 5×5 matrix, namely 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120.

As a corollary to the proof of the theorem we have the following.

COROLLARY. Let G be a group of order $p^m s$ (p and s relatively prime), and let f be a representation of G by non-singular $n \times n$ rational matrices, where $n < p - 1$. Then the order of the kernel H of the representation is divisible by p^m.

Proof. The representation f induces a faithful representation $\bar{f}$ of G/H. If the order of H is not divisible by p^m then the prime p divides the order of G/H. Let a be an element of order p in G/H (1, p. 43), then $\bar{f}(a)$ has order p which is a contradiction.

REFERENCES

1. Marshall Hall, Jr., The Theory of Groups. Macmillan, 1959.

2. J. Barkley Rosser and Lowell Schoenfeld, Approximate Formulas for some Functions of Prime Numbers. Illinois Journal of Mathematics, Vol. 6, No. 1, March, 1962, 64-94.

3. O. Schreier and E. Sperner, Modern Algebra and Matrix Theory. Chelsea, 1955.

4. B. L. van der Waerden, Modern Algebra, Vol. 1, Ungar, 1953.

Temple University

https://doi.org/10.4153/CMB-1967-044-x Published online by Cambridge University Press