CONCERNING AN EQUIVALENCE RELATION FOR MATRICES

EMANUEL VEGH
U.S. Naval Research Laboratory, Washington, D.C., and Imperial College, London SW 7

Let each of s and n be a positive integer, p an arbitrary prine, Λ the field of integers modulo p and S the set of all s by n matrices over Λ. Let each of A and B be in S. We say that A is equivalent to B (written $A \sim B$) if and only if there is a non-singular matrix X over Λ and a matrix $Y = (y_{ij})$ in S with

$$y_{i1} \equiv y_{i2} \equiv \cdots \equiv y_{in} \pmod p, \qquad i = 1, 2, \cdots, s$$

such that

$$A = XB + Y.$$

It is easy to show that $\sim$ is an equivalence relation on S. Let $L_p(s,n)$ be the smallest non-negative number not greater than $p - 1$ such that each equivalence class contains a member $X = (x_{ij})$ with the property that

$$0 \leqslant x_{ij} \leqslant L_p(s,n) \qquad 1 \leqslant i \leqslant s, \qquad 1 \leqslant j \leqslant n.$$

We shall give an elementary proof of the

Theorem.

$$L_p(s,n) \leqslant 2[p^{(ns-t-1)/(ns-t)}], \qquad n = 2, 3, \cdots ,$$

where

(1) $$t = s^2 \text{ if } s \leqslant [n/2] \quad \text{and} \quad t = [n/2]^2 - n[n/2] + ns \text{ if } s > [n/2].$$

Here $[x]$ is the greatest integer $\leqslant x$.

For the case $s = 1$ the theorem gives

$$L_p(1,n) \leqslant 2[p^{(n-2)/(n-1)}], \qquad n = 2, 3, \cdots .$$

L. Redei [3] has shown, using the geometry of numbers, that

$$L_p(1,n) \leqslant 2n^{-1/(n-1)}p^{(n-2)/(n-1)}, \qquad n = 2, 3, \cdots .$$

Using elementary methods (a theorem of Thue [4]), Redei has also shown that

$$L_p(1,n) \leqslant 2([p^{1/(n-1)}] + 1)^{n-2}, \qquad n = 2, 3, \cdots .$$

Our theorem then generalizes the results of Redei and improves his weaker inequality, by elementary methods.

We shall make use of the following theorem which has an elementary proof.

Theorem A. (A. Brauer and R.L. Reynolds [1]). Let r and s be rational integers $r < s$ and let f_δ be positive numbers less than m $(\delta = 1, 2, \cdots, s)$ such that

$$\prod_{\delta=1}^{s} f_\delta > m^r .$$

Then the system of r linear congruences

$$y_\rho = \sum_{\delta=1}^{s} a_{\rho\delta} x_\delta \equiv 0 \pmod m \qquad (\rho = 1, 2, \cdots, r)$$

has a non-trivial solution in integers $x_1, x_2, \cdots, x_s$ such that

$$|x_\delta| < f_\delta \qquad (\delta = 1, 2, \cdots, s) .$$

We note that the hypothesis of this theorem can be weakened by letting the numbers f_δ $(\delta = 1, 2, \cdots, s)$ be positive numbers *not greater than* m. The proof is the same as in [1]. We follow, in part, the method of Redei [3], as given when $s = 1$.

Now let $Y = (y_{ij})$ be a member of S. The matrix $Z = (z_{ij})$, where $Z = IY + B$, I is the identity matrix and $B = (b_{ij})$ is the matrix with

$$b_{i1} = b_{i2} = \cdots = b_{in} = -y_{in} \qquad (i = 1, 2, \cdots, s),$$

is equivalent to Y. Note that $z_{in} = 0$, $i = 1, 2, \cdots, s$.

Let r be the rank of the matrix Z. It is well known that there is a non-singular matrix C over Λ, such that the matrix $U = CZ$ has $s - r$ zero rows and has r columns each with exactly one non-zero element (see for example [2]). The matrix U then has at least

$$f(r) = r^2 - nr + ns, \qquad 0 \leqslant r \leqslant s$$

zero elements. The minimum value for $f(r)$ is given by t in (1). Thus Y is equivalent to a matrix U that has at most $ns - t$ non-zero elements.

Let $u_1, u_2, \cdots, u_\lambda$ be the non-zero elements of U. Consider the system

(2) $$x_i \equiv au_i \pmod p, \qquad i = 1, 2, \cdots, \lambda$$

of λ congruences in the $\lambda + 1$ variables a, x_i $(i = 1, 2, \cdots, \lambda)$. Setting $f_0 = p$ and $f_\delta = [p^{(\lambda-1)/\lambda}] + 1$, $(\delta = 1, 2, \cdots, \lambda)$, we have

(3) $$\prod_{\delta=0}^{\lambda} f_\delta = p([p^{(\lambda-1)/\lambda}] + 1)^\lambda > p(p^{(\lambda-1)/\lambda})^\lambda = p^\lambda .$$

Using Theorem A, the remark following it, together with (3), it follows that the system of linear congruences (2) has a non-trivial solution a, x_i $(i = 1, 2, \cdots, \lambda)$ with

$$|a| \leqslant p - 1 \qquad \text{and} \qquad |x_i| \leqslant [p^{(\lambda-1)/\lambda}], \qquad i = 1, 2, \cdots, \lambda .$$

Since the solution is non-trivial, $a \not\equiv 0 \pmod p$; and since $\lambda \leqslant ns - t$,

(4) $$|x_i| \leqslant [p^{(ns-t-1)/(ns-t)}], \qquad i = 1, 2, \cdots, \lambda .$$

The s by n matrix $X = (x_{ij})$ with entries x_i $(i = 1, 2, \cdots, \lambda)$ in the same position as u_i $(i = 1, 2, \cdots, \lambda)$ of U, and zero elsewhere, satisfies the equation $X = AU$, where A is the diagonal matrix with all diagonal entries equal to a. Naturally, since $a \not\equiv 0 \pmod p$, A is non-singular.

Set

$$t = \max_{i,j} |x_{ij}| .$$

If T is the s by n matrix all of whose entries are t, then $W = (w_{ij})$, where $W = IX + T$ is equivalent to X, and

(5) $$0 \leqslant w_{ij} \leqslant 2[p^{(ns-t-1)/(ns-t)}], \qquad 1 \leqslant i \leqslant s, \quad 1 \leqslant j \leqslant n .$$

Since $Y \sim W$, we have, using (5) together with the definition of $L_p(s,n)$, proved the theorem.

REFERENCES

1. A. Brauer and R.L. Reynolds, "On a Theorem of Aubry-Thue," *Can. J. Math.,* Vol. 3 (1951), pp. 367–374.
2. S. Perlis, *Theory of Matrices,* Addison-Wesley, Reading, Mass., 1958.
3. L. Redei, "Über Eine Verschärfung Eines Zahlentheoretischen Satzes Von Thue," *Acta Math. Acad. Sci. Hungar,* 2 (1951), pp. 75–82.
4. A. Thue, "Et par antydninger til en taltheoretisk methode," *Christiania Videnskabs Selakabs Forh.,* 1902, No. 7, S. 1–21.

****