L. A. GUTNIK

1958

SovietRxiv

Abstract

Full Text

L. A. GUTNIK

ON THE ARITHMETIC OF MATRICES

(Presented by Academician I. M. Vinogradov on 8 IV 1958)

Let the group of all integral matrices of order n with determinant congruent modulo to 1 be denoted by U_n. A diagonal matrix δ of order n is called an ET-matrix if it is diagonal,

$$\delta_{i;i} > 0, \quad i = 1, \dots, n; \qquad \delta_{i;i} \mid \delta_{i+1;i+1}, \quad i = 1, \dots, n-1. \tag{1}$$

The determinant of a matrix α is denoted by $D(\alpha)$; the matrix transposed to α is denoted by α'. For denoting zero matrices the letter ω is reserved, and for denoting identity matrices—the letter ε. Let α be a matrix of order n; let ε and ω be, respectively, the identity and zero matrices of order n. The symbol α^A denotes the matrix

$$\begin{pmatrix} \omega & \alpha \\ -\alpha' & \omega \end{pmatrix},$$

and the symbol α^B denotes the matrix

$$\begin{pmatrix} \varepsilon & \omega \\ \omega & \alpha \end{pmatrix}.$$

Let α be an arbitrary integral nonsingular matrix of order n. Using the theorem on elementary divisors, it is easy to show that in the set $U_n \alpha U_n$ there lies one and only one ET-matrix; this ET-matrix, invariantly associated with the matrix α, is called the E-form of the matrix α and is denoted by α^E. Let π be an integral nonsingular skew-symmetric matrix of order $2n$. From the well-known theorem of Jacobi it follows that in the set $U_{2n} \pi U_{2n}$ there lies one and only one matrix of the form δ^A, where δ is an ET-matrix; this matrix of the form δ^A, invariantly associated with the matrix π, is called the ES-form of the matrix π and is denoted by π^{ES}.

Let α be an integral nonsingular matrix of order n. An integral nonsingular matrix β is called an element of a left (right) divisor of the matrix α, if the matrix $\beta^{-1}\alpha$ (the matrix $\alpha\beta^{-1}$) is integral. If β is an element of a left (right) divisor of the matrix α, then (see (3)) $\beta^E \mid \alpha^E$. If β is an element of a left (right) divisor of the matrix α, $\nu \in \Omega_n$, then the matrix $\beta\nu$ (the matrix $\nu\beta$) is also an element of a left (right) divisor of the matrix α. Therefore the set of matrices associated on the right (on the left) with respect to the group U_n with some element of a left (right) divisor of the matrix α consists entirely of elements of a left (right) divisor of the matrix α; this set we shall call a left (right) divisor

of the matrix α. It is easily proved that the set of left (right) divisors of the matrix α is finite and contains no more than $D^n(\alpha)$ elements. The number of left (right) divisors of the matrix α will be denoted by $t_l(\alpha)$ (by $t_r(\alpha)$). It is obvious that the matrices belonging to a certain left (right) divisor of the matrix α have one and the same E-form. The number of left (right) divisors of the matrix α having one and the same E-form γ will be denoted by $t_l(\alpha, \gamma)$ (by $t_r(\alpha, \gamma)$). From (1) it follows that

$$t_l(\alpha) = \sum_{\gamma|\alpha^E} t_l(\alpha, \gamma), \qquad t_r(\alpha) = \sum_{\gamma|\alpha^E} t_r(\alpha, \gamma). \tag{2}$$

Using the operation of transposition, it is easy to show that

$$t_l(\alpha, \gamma) = t_r(\alpha', \gamma). \tag{3}$$

Further, it is not difficult to show that

$$t_l(\alpha, \gamma) = t_l(\alpha^E, \gamma), \qquad t_r(\alpha, \gamma) = t_r(\alpha^E, \gamma). \tag{4}$$

Comparing (3) and (4), we obtain

$$t_l(\alpha, \gamma) = t_r(\alpha, \gamma), \qquad t_l(\alpha) = t_r(\alpha). \tag{5}$$

In view of (5), put $t(\alpha, \gamma) = t_l(\alpha, \gamma) = t_r(\alpha, \gamma)$, $t(\alpha) = t_l(\alpha) = t_r(\alpha)$. Then (2) gives

$$t(\alpha) = \sum_{\gamma|\alpha^E} t(\alpha, \gamma). \tag{6}$$

It is natural to call the function $t(\alpha)$ the **number of divisors of the matrix** α: in the case when α is a matrix of the first order, $t(\alpha)$ is equal to the number of divisors of the modulus of the number α. In view of (4), in studying the functions $t(\alpha)$ and $t(\alpha, \gamma)$ one may restrict oneself to matrices α that are ET-matrices.

Let a be a nonzero integer; p a prime number; by $a^{[p]}$ denote the highest integral power of p dividing a. Let δ be an ET-matrix of order n; p a prime number; by $\delta^{[p]}$ denote the ET-matrix having diagonal elements $\delta^{[p]}_{1;1}, \ldots, \delta^{[p]}_{n;n}$. Then every ET-matrix δ is represented uniquely in the form $\delta = \prod_{p|D(\delta)} \delta^{[p]}$. Let γ and δ be ET-matrices of order n; p a prime number. Introduce the following symbols: $e^{[p]}(\gamma)$ is the number of elements of the sequence $\gamma^{[p]}_{1;1}, \ldots, \gamma^{[p]}_{n;n}$ equal to 1; ${}^{[p]}_{i}(\delta, \gamma)$ is the number of elements of the sequence $\delta^{[p]}_{1;1}, \ldots, \delta^{[p]}_{n;n}$ not smaller than $\gamma^{[p]}_{i;i}$;

${}_i^{[p]}(\delta,\gamma)$ is the number of elements of the sequence $\delta_{1;1}^{[p]},\dots,\delta_{n;n}^{[p]}$ greater than $\gamma_{i;i}^{[p]}$; ${}_i^{[p]}(\delta,\gamma)$ is the number of elements of the sequence $\delta_{j;j}^{[p]}$, $i\le j\le n$, equal to $\gamma_{i;i}^{[p]}$.

Theorem 1.

$$t(\delta,\gamma)=$$

$$=\prod_{p|D(\delta)}\prod_{i=1}^{n}\left(\gamma_{i;i}^{[p]}\right)^{-{}_i^{[p]}(\delta,\gamma)+\mathrm{E}_i^{[p]}(\gamma,\gamma)-{}_i^{[p]}(\gamma,\gamma)}\left(\delta_{i;i}^{[p]}\right)^{{}_i^{[p]}(\gamma,\delta)}\frac{1-p^{{}_i^{[p]}(\delta,\gamma)-i}}{1-p^{{}_i^{[p]}(\gamma,\gamma)-i}}. \qquad (7)$$

Let π,ρ be two integral, nonsingular, skew-symmetric matrices of order $2n$. Denote by $A_0(\pi,\rho)$ the set of all integral matrices χ satisfying the relation $\chi'\pi\chi=\rho$. Clearly, the set $A_0(\pi,\pi)$ is a group. If $\mu\in A_0(\pi,\pi)$, $\nu\in A_0(\rho,\rho)$, then $\mu A_0(\pi,\pi)\nu=A_0(\rho,\rho)$. The quotient space of the set $A_0(\pi,\rho)$ with respect to the group of automorphisms $A_0(\pi,\rho)\to\mu A_0(\pi,\rho)$, $\mu\in A_0(\pi,\pi)$, will be denoted by $L_0(\pi,\rho)$. The quotient space of the set $A_0(\pi,\rho)$ with respect to the group of automorphisms $A_0(\pi,\rho)\to A_0(\pi,\rho)\nu$, $\nu\in A_0(\rho,\rho)$, will be denoted by $R_0(\pi,\rho)$. It is easily proved that the sets $L_0(\pi,\rho)$ and $R_0(\pi,\rho)$ are finite and that the number of elements of each of them does not exceed $\left(D(\rho\pi^{-1})\right)^{2n^2}$. Denote the number of elements of the set $L_0(\pi,\rho)$ by $a_l(\pi,\rho)$, and the number of elements of the set $R_0(\pi,\rho)$ by $a_r(\pi,\rho)$. Then it is not difficult to show that $a_l(\pi,\rho)=a_l(\pi^{ES},\rho^{ES})$, $a_r(\pi,\rho)=a_r(\pi^{ES},\rho^{ES})$. Therefore, in studying the numbers $a_l(\pi,\rho)$ and $a_r(\pi,\rho)$ one may restrict oneself to matrices π and ρ having the form $\pi=\gamma^A$, $\rho=\delta^A$, where γ and δ are ET-matrices.

Theorem 2. Let ε be the identity matrix of order n, and let δ be an ET-matrix of order n. Then

$$a_l(\varepsilon^A,\delta^A)=\sum_{\gamma|\delta}t(\delta,\gamma)\prod_{i=1}^{n}\gamma_{i;i}^{n-i+1},$$

where the sum is extended over all ET-matrices γ for which the matrix $\gamma^{-1}\delta$ is integral.

Let A be a group, and B a subgroup of finite index of the group A. By $[A:B]$ we denote the index of the subgroup B in the group A. Put $A(\gamma,\delta)=\gamma^B A_0(\gamma^A,\delta^A)(\delta^B)^{-1}$, $M(\gamma)=A(\gamma,\gamma)$. It is easy to see that $M(\gamma)$ is a subgroup of the symplectic group. As was shown by Kézher ([4]),

$$\frac{a_r(\gamma^A,\delta^A)}{a_l(\gamma^A,\delta^A)}=\frac{[M(\gamma):K(\gamma,\delta)]}{[M(\delta):K(\gamma,\delta)]},$$

where $K(\gamma,\delta)=M(\gamma)\cap M(\delta)$.

Theorem 3.

$$\frac{[M(\gamma):K(\gamma,\delta)]}{[M(\delta):K(\gamma,\delta)]}=\prod_{p|D(\gamma\delta)}\frac{\prod_{i=1}^{n}(\gamma_{i;i}^{[p]})^{2n-4i+2}\left(1-\frac{1}{p^{\mathfrak{e}_i^{[p]}(\gamma,\gamma)}}\right)}{\prod_{i=1}^{n}(\delta_{i;i}^{[p]})^{2n-4i+2}\left(1-\frac{1}{p^{\mathfrak{e}_i^{[p]}(\delta,\delta)}}\right)}. \tag{9}$$

Let π and ρ be two integral nonsingular skew-symmetric matrices of order $2n$; q_1 and q_2 two natural numbers. We divide the set of matrices satisfying the congruence $\chi'\pi\chi\equiv\rho\pmod{q_1}$ into classes, assigning to one class matrices congruent to one another modulo q_2. We denote the number of classes obtained by $N_{q_1,q_2}(\pi,\rho)$.

Theorem 4. Let δ be an ET-matrix of order n; p a prime number; b a natural number satisfying the requirement

$$p^b>\delta_{n;n}^{[p]}. \tag{10}$$

Then

$$N_{p^b,p^b}(\delta^A,\delta^A)=p^{bn(2n+1)}\prod_{i=1}^{n}(\delta_{i;i}^{[p]})^{4n-4i+1}\left(1-\frac{1}{p^{\mathfrak{e}_i^{[p]}(\delta,\delta)}}\right). \tag{11}$$

For $\delta=\varepsilon$, from formula (10) there follows the well-known fact

$$N_{p^b,p^b}(\varepsilon^A,\varepsilon^A)=p^{bn(2n+1)}\prod_{i=1}^{n}\left(1-\frac{1}{p^{2i}}\right). \tag{12}$$

Theorem 5. Let δ be an ET-matrix of order n; p a prime number; b,c natural numbers subject to the requirement $p^b(\delta_{n;n}^{[p]})^{-1}>p^c>\delta_{n;n}^{[p]}$. Then

$$N_{p^b,p^c}(\delta^A,\delta^A)=p^{cn(2n+1)}\prod_{i=1}^{n}(\delta_{i;i}^{[p]})^{2n-4i+2}\left(1-\frac{1}{p^{\mathfrak{e}_i^{[p]}(\delta;\delta)}}\right). \tag{13}$$

From formula (11) it follows that, when inequality (10) is satisfied, the quantity $N_{p^b,p^b}(\delta^A,\delta^A)/p^{bn(2n+1)}$ does not depend on b.

Using an idea of Siegel, one can prove the following general fact.

Theorem 6. Let π,ρ be two integral nonsingular matrices of order $2n$; p a prime number; p^{b_0} the highest integral power entering into the determinant of the matrix ρ; b an integer satisfying the requirement $b>2b_0$. Then the number $N_{p^b,p^b}(\pi,\rho)p^{-bn(2n+1)}$ does not depend on the number b.

We denote this number independent of b by $c_p(\pi, \rho)$. Let ρ be a nonsingular skew-symmetric matrix of order $2n$. By $\Psi(\rho)$ we denote some neighborhood of the matrix ρ, consisting of skew-symmetric matrices of order $2n$. If $\psi \in \Psi(\rho)$, then the elements $\psi_{k,l}$, $1 \leq k < l \leq 2n$, are regarded as independent rectangular coordinates in an $n(2n-1)$-dimensional Euclidean space. Let π also be some nonsingular skew-symmetric matrix of order $2n$. By $\Omega(\pi, \Psi)$ we denote the set of all real matrices satisfying the requirement $\xi' \pi \xi \in \Psi$.

If $\xi \in \Omega(\pi, \Psi)$, the elements $\xi_{i,j}$, $i, j = 1, \ldots, 2n$, will be regarded as independent rectangular coordinates in $4n^2$-dimensional Euclidean space. It is easy to see that if $\mu \in A_0(\pi, \pi)$, then

$$\mu\Omega(\pi, \Psi) = \Omega(\pi, \Psi).$$

It can be proved that if the diameter of the domain $\Psi(\rho)$ is sufficiently small, then there exists a fundamental domain $\Omega_0(\pi, \Psi)$ of the space $\Omega(\pi, \Psi)$ with respect to its automorphism group $\Omega(\pi, \Psi) \to \mu\Omega(\pi, \Psi)$, $\mu \in A_0(\pi, \pi)$, having finite volume. Let M be some set having finite volume; then the volume of the set M is denoted by $v(M)$. It can be shown that if the neighborhood $\Psi(\rho)$ is contracted to the point ρ, then the ratio

$$v(\Omega_0(\pi, \Psi))/v(\Psi(\rho))$$

tends to a certain finite nonzero limit, which we denote by $c_0(\pi, \rho)$. Since, if p does not divide $D(\pi\rho)$, then

$$c_p(\pi, \rho) = \prod_{i=1}^{n} \left(1 - \frac{1}{p^{2i}}\right),$$

it is easy to see that the product

$$\prod_{(p, D(\pi\rho))=1} c_p(\pi, \rho),$$

extended over all prime numbers not entering into the determinant $D(\pi, \rho)$, converges. We denote by

$$\prod_{p} c_p(\pi, \rho)$$

the quantity

$$\prod_{(p, D(\pi\rho))=1} c_p(\pi, \rho) \prod_{p | D(\pi\rho)} c_p(\pi, \rho).$$

In Theorem 7 there is proved a statement asserted by I. I. Pjateckii-Shapiro.

Theorem 7.

$$a_1(\pi, \rho) = c_0(\pi, \rho) \prod_{p} c_p(\pi, \rho). \tag{14}$$

The proof of Theorem 7 is easily reduced to the case when $\pi = \gamma^A$, $\rho = \delta^A$. Siegel [2] showed that

$$1 = c_0(\varepsilon^A, \varepsilon^A) \prod_p c_p(\pi, \rho). \tag{15}$$

Using (9), we find an expression for $c_0(\delta^A, \delta^A)/c_0(\varepsilon^A, \varepsilon^A)$; comparing it with (11), (12), and (15), we obtain the proof of Theorem 7 for the case when $\pi = \rho$; from the result thus obtained, applying Siegel' s method, developed by him in [1], we derive relation (14). Relation (14) may be regarded as an analogue of Siegel' s theorem on quadratic forms [1]. From Theorems 7, 3, and 6 follow Theorems 8 and 9.

Theorem 8. Let γ, δ be matrices of order n. Then

$$a_1(\gamma^A, \delta^A) = \prod_{p|D(\gamma\delta)} a_1((\gamma^{[p]})^A, (\delta^{[p]})^A, (\rho^{[p]})^A),$$

$$a_r(\gamma^A, \delta^A) = \prod a_r((\gamma^{[p]})^A, (\delta^{[p]})^A).$$

Theorem 9. Let π, ρ be two nonsingular skew-symmetric matrices of order $2n$; let q be a natural number; $D^3(\pi\rho)\backslash q$. Then an integral matrix χ satisfying the relation

$$\chi'\pi\chi = \rho$$

exists if and only if the congruence

$$\chi'\pi\chi \equiv \rho \pmod{q}$$

is solvable.

Theorem 9 may be regarded as an analogue of the well-known Hasse theorem on quadratic forms.

In conclusion I express my sincere gratitude to Prof. A. A. Buchstab for his attention to the present work.

Received
3 IV 1958

References

[1] C. L. Siegel, Ann. Math., **36**, 527 (1935).
[2] C. L. Siegel, Am. J. Math., **65**, 1, (1943).
[3] M. Koecher, Math. Nachr., **13**, 367 (1955).
[4] M. Koecher, Math. Ann., **130**, H. 5, 351, (0a) (1956).

Note: Figure translations are in progress. See original paper for figures.