Representations by bilinear forms (mod. p^a)

by JOHN H. HODGES (in Boulder, Colorado, U.S.A.) (*)

In memory of Guido Castelnuovo, in the recurrence of the first centenary of his birth.

Summary. - *An expression is derived for the number of representations of one bilinear form by another (mod p^a). From this, an explicit formula for the number of such representations is obtained in the case where both forms have square nonsingular matrices (mod p). A related bilinear analog of a lemma of Siegel on representations by quadratic forms (mod p^a) is also proved.*

1. - Introduction and preliminaries.

Let A and B be $m \times n$ and $s \times t$ matrices, respectively, with integral elements. For an arbitrary prime integer p and any positive integer a , let $N(A, B, a)$ denote the number of incongruent solutions U, V of the congruence

$$(1.1) \quad UAV \equiv B \pmod{p^a},$$

where U and V are integral $s \times m$ and $n \times t$ matrices, respectively. If f and g are bilinear forms (mod p^a) in $m + n$ and $s + t$ variables with coefficient matrices A and B , respectively, then $N(A, B, a)$ is the number of «representations» of g by f (mod p^a).

For $a = 1$, that is, for bilinear forms over the prime finite field $GF(p)$, $N(A, B, a)$ is given explicitly [1; Theorem 3 with $q = p$] as

$$(1.2) \quad N(A, B, 1) = p^{ms + nt - st - z(2r - z + 1)/2} \cdot \prod_{i=0}^{z-1} (p^{r-i} - 1),$$

$$\sum_{j=0}^{\min(s-z, t-z)} p^{-(r-z)j} g(s-z, t-z, j),$$

where (mod p) rank $A = r$ and rank $B = z$ and $g(s, t, j)$, the number of $s \times t$ matrices of rank j (mod p) is given by the formula, due to LANDSBERG [3],

$$(1.3) \quad g(s, t, j) = p^{j(j-1)/2} \prod_{i=1}^j \frac{(q^{s-i+1} - 1)(q^{t-i+1} - 1)}{(q^i - 1)}.$$

(*) Research supported by National Science Foundation Grants GP-2542 and GP-4015.

We extend this definition by taking $g(0, 0, 0) = 1$.

In the present paper, we shall consider the case $a > 1$ of (1.1). First (Theorem 1), an expression is obtained for $N(A, B, k+1)$, for all $k \geq 1$, as a complicated multiple sum involving the numbers of solutions of certain linear matrix congruences (mod p) in two unknowns. These linear congruences are associated with the solutions of (1.1) with $a = k$ and are special cases of linear matrix equations over a finite field which were considered by the writer in [2; § 6]. Then (Theorem 2) in the particular case of (1.1) where A and B are both square and nonsingular (mod p), by using Theorem 1 and the value of $N(A, B, 1)$ given by (1.2), the explicit value of $N(A, B, k+1)$ is found for all $k \geq 1$. The result in Theorem 2 is the bilinear analog of some special cases of results of SIEGEL [5] on representations by quadratic forms (mod p^a). Finally, we establish (Theorem 3) for A and B square and $|B| \not\equiv 0$, a recursion formula for $N(A, B, k)$ for k sufficiently large, which is the general bilinear analog of a lemma of SIEGEL [5; Lemma 13].

Except as indicated, Roman capitals in this paper will denote matrices with integral elements. In particular $I(m, t; r)$ will denote the $m \times t$ matrix with the identity of order r in its upper left hand corner and zeros elsewhere and $I_t = I(t, t; t)$, the identity of order t .

2. - The congruence (1.1) for $a > 1$.

If we attempt to construct all incongruent solutions of (1.1) for $a = k+1$ with $k \geq 1$ by using solutions of (1.1) for $a = k$ we are led to

THEOREM 1. - *For all $k \geq 1$, the number $N(A, B, k+1)$ of incongruent solutions U, V of the congruence (1.1) with $a = k+1$ is*

$$(2.1) \quad N(A, B, k+1) = \sum_{v=0}^c \sum_{u=0}^d p^{e(u,v)} \sum_{U_k A V_k \equiv B \pmod{p^k}} h(s-u, t-v, W_k),$$

where $c = \min(m, t)$, $d = \min(s, n)$, $e(u, v) = s(m-v) + t(n-u) + uv$; the inner summation is over all incongruent solutions U_k, V_k of (1.1) for $a = k$ such that if $U_k \equiv U_i, V_k \equiv V_i \pmod{p}$, then there exist nonsingular matrices (mod p) P, Q, E, F of the appropriate sizes such that $PAV_i Q \equiv I(m, t; v)$ and $EU_i A F \equiv I(s, n; u) \pmod{p}$; for any such P, Q, E, F , $W_k = p^{-k} E(B - U_k A V_k) Q$ and $h(s-u, t-v, W_k) = 0$ or 1 as defined in (2.5).

PROOF. - Let U_k, V_k be an arbitrary solution of (1.1) with $a = k$ and suppose that $U_k \equiv U_i, V_k \equiv V_i \pmod{p}$. Then a pair of integral matrices U_{k+1}, V_{k+1} satisfy (1.1) with $a = k+1$ and have the properties

$$U_{k+1} \equiv U_k \pmod{p^k}, \quad V_{k+1} \equiv V_k \pmod{p^k},$$

if and only if

$$(2.2) \quad U_{k+1} = U_k + p^k R, \quad V_{k+1} = V_k + p^k T,$$

where R and T are integral matrices such that

$$U_k A V_k + p^k (U_k A T + R A V_k) \equiv B \pmod{p^{k+1}},$$

or equivalently

$$(2.3) \quad R A V_k + U_k A T \equiv p^{-k} (B - U_k A V_k) \pmod{p}.$$

Let P, Q, E, F be any nonsingular matrices (mod p) of the appropriate sizes such that

$$P A V_1 Q \equiv I(m, t; v) \quad \text{and} \quad E U_1 A F \equiv I(s, n; u) \pmod{p},$$

and $W_k = p^{-k} E (B - U_k A V_k) Q = (w_{ij})$. Then the number of incongruent solutions $R, T \pmod{p}$ of (2.3), so equivalently the number of incongruent solutions U_{k+1}, V_{k+1} of (1.1), with $a = k + 1$, which are congruent (mod p^k) to U_k, V_k , respectively, is given in [2; Theorem 7] as

$$(2.4) \quad p^{e(u, v)} h(s - u, t - v, W_k),$$

where $e(u, v) = s(m - v) + t(n - u) + uv$ and

$$(2.5) \quad h(s - u, t - v, W_k) = \begin{cases} 1 & \text{if } w_{ij} = 0 \text{ all } u < i \leq s \text{ and } v < j \leq t, \\ 0 & \text{otherwise.} \end{cases}$$

Also, $h(s - u, t - v, W_k) = 1$ if $u = s$ or $v = t$.

In view of the remarks in the preceding paragraph, if we sum (2.4) over all incongruent solutions U_k, V_k of (1.1) for $a = k$ and group together in the resulting sum the contributions corresponding to all such U_k, V_k which lead to the same values of v, u with $0 \leq v \leq c = \min(m, t)$ and $0 \leq u \leq d = \min(s, n)$, then we obtain (2.1).

3. - A special case of (1.1).

Of particular interest is the special case of (1.1) where both A and B are square and nonsingular (mod p), that is, $s = t$ with $|B| \not\equiv 0 \pmod{p}$ and $m = n$ with $|A| \not\equiv 0 \pmod{p}$. Since no solutions of (1.1) exist otherwise, we may assume in this case that $t \leq m$. Using Theorem 1 in this case along with (1.2) we get

THEOREM 2. - For all $k \geq 0$, the number $N(A, B, k+1)$ of incongruent solutions U, V of the congruence (1.1) with $a = k+1$, where A and B are square and nonsingular (mod p) of orders m and t , respectively, is

$$(3.1) \quad N(A, B, k+1) = p^{t[k(2m-t)+m]-t(t+1)/2} \prod_{i=0}^{t-1} (p^{m-i} - 1)$$

PROOF. - Taking $m = n = r$ and $s = t = z$ in (1.2), we see that for A and B as above

$$(3.2) \quad N(A, B, 1) = p^{t(2m-t-1)/2} \prod_{i=0}^{t-1} (p^{m-i} - 1),$$

which is (3.1) with $k = 0$.

Suppose now that $k \geq 1$. Since B is nonsingular (mod p), all solutions U_i, V_i of (1.1) with $a = 1$ must have (mod p) ranks equal to t . Since A is also nonsingular (mod p), then AV_i and U_iA must also have (mod p) ranks equal to t . Thus $v = u = t$ in the notation of Theorem 1. Therefore, corresponding to each incongruent solution U_k, V_k of (1.1) with $a = k$, we have $v = t = s = u$ so that by definition $h(s-u, t-v, W_k) = 1$. Since in this case, $e(u, v) = e(t, t) = t(2m-t)$, it follows from (2.1) that

$$(3.3) \quad N(A, B, k+1) = p^{t(2m-t)} N(A, B, k).$$

Applying the recursion formula (3.3) k times and using the explicit value of $N(A, B, 1)$ given by (3.2) we obtain (3.1).

We note that the result in Theorem 2 is the bilinear analog of some results of SIEGEL [5; Lemmas 12 and 13, the latter in the special case $p \nmid 2ST$] on representations by quadratic forms (mod p^a).

4. - Bilinear analog of a lemma of Siegel.

In this section we prove a theorem of a slightly different sort, which is the general bilinear analog of the second of the two lemmas of SIEGEL referred to in § 3 [5; Lemma 13]. By use of a method analogous to that used by SIEGEL, we prove

THEOREM 3. - Let A and B be square of orders m and t , respectively, with $t \leq m$. If p^b is the highest power of p which divides $|B|$, then for any $k > 2b$ the number $N(A, B, k)$ of incongruent solutions U, V of the congruence (1.1) with $a = k$ satisfies

$$(4.1) \quad (p^{k+1})^{t^2-2mt} N(A, B, k+1) = (p^k)^{t^2-2mt} N(A, B, k).$$

That is, with $q = p^k$, $q^{t^2-2mt}N(A, B, k)$ is independent of k .

PROOF. - We first note that in general in (1.1) we may assume without any real loss of generality that A is square. For otherwise, by means of linear transformations of U and V with integral matrices of determinant ± 1 , A may be transformed [4; Theorem 26.2] into diagonal form so that (1.1) reduces to a congruence of the same form involving submatrices of U and V , but in which the matrix corresponding to A is diagonal and square.

Now let U_k, V_k be a solution of (1.1) with $a = k$. Let $n(U_k, V_k)$ denote the number of incongruent solutions U, V of (1.1) with $a = k$ such that $U \equiv U_k, V \equiv V_k \pmod{p^{k-b}}$. Then U, V is such a solution of (1.1) if and only if

$$U = U_k + p^{k-b}X \quad \text{and} \quad V = V_k + p^{k-b}Y,$$

where

$$(4.2) \quad XAV_k + U_kAY \equiv 0 \pmod{p^b}.$$

Thus, $n(U_k, V_k)$ is the number of incongruent (mod p^b) solutions X, Y of (4.2). Furthermore, such a pair U, V is a solution of (1.1) with $a = k + 1$ if and only if

$$(4.3) \quad XAV_k + U_kAY \equiv W_k \equiv p^b[p^{-k}(B - U_kAV_k)] \pmod{p^{b+1}}.$$

By [4; Theorem 26.2] there exist square integral matrices P, Q, E, F of the appropriate orders having determinants equal to ± 1 and such that

$$(4.4) \quad PAV_kQ = \text{col}(C, 0), \quad EU_kAF = (D, 0),$$

where $C = \text{diag}(c_1, \dots, c_t)$, $D = \text{diag}(d_1, \dots, d_t)$ and all c_j and d_i are integers. Suppose that $c_j = 0$ for some $1 \leq j \leq t$. Then over the rational field, $\text{rank}(AV_k) < t$ so that $\text{rank}(U_kAV_k) < t$ and so

$$0 = |U_kAV_k| \equiv |B| \pmod{p^k},$$

which is contradictory to the hypothesis, since $k > b$. Therefore, $c_j \neq 0$ all $1 \leq j \leq t$ so that C^{-1} exists over the rational field. Likewise, $d_i \neq 0$ all $1 \leq i \leq t$ and D^{-1} exists over the rationals. Furthermore, also over the rationals,

$$U_kAV_kQC^{-1} = U_kP^{-1}(PAV_kQ)C^{-1} = U_kP^{-1}\text{col}(I_t, 0)$$

has integral elements, where I_t denotes the identity matrix of order t . This implies that $|U_kAV_k| = h|C|$ so that

$$|U_kAV_k| \equiv |B| \equiv h|C| \pmod{p^k},$$

where h is an integer. Thus, if p^g is the highest power of p which divides any c_j for $1 \leq j \leq t$, then $g \leq b$. Similarly if p^f is the highest power of p which divides any d_i for $1 \leq i \leq t$, then $f \leq b$.

Now if we make the substitutions $X_0 = EXP^{-1} = (X_1, X_2)$, $Y_0 = F^{-1}YQ = \text{col } (Y_1, Y_2)$ and $W_0 = EW_kQ$, where X_1 and Y_1 are square of order t , then we see that (4.2) and (4.3) are equivalent to

$$(4.5) \quad X_2, Y_2 \text{ arbitrary, } X_1 C + D Y_1 \equiv W_0 \pmod{p^e},$$

where $e = b$ and $e = b + 1$, respectively, and $W_0 \equiv 0 \pmod{p^b}$. If we let $X_1 = (x_{ir})$, $Y_1 = (y_{sj})$ and $W_0 = (w_{ij})$, and recall that C and D are diagonal matrices, the matrix congruence in (4.5) is equivalent to

$$(4.6) \quad x_{ij}c_j + d_i y_{ij} \equiv w_{ij} \pmod{p^e} \quad (1 \leq i, j \leq t),$$

a system of t^2 congruences in the $2t^2$ unknowns x_{ij}, y_{ij} .

For any choice of i and j , $1 \leq i, j \leq t$, suppose that p_{ij} is the highest power of p dividing (d_i, c_j) so that, by what was shown above, p_{ij} divides d^e . Without loss of generality, we may suppose that p_{ij} is the highest power of p which divides c_j . Since both the right member and the modulus of the congruence

$$c_j x_{ij} \equiv w_{ij} - d_i y_{ij} \pmod{p^e}$$

are divisible by p_{ij} , clearly $p_{ij} = (c_j, p^e)$ and for each of the arbitrary choices of $y_{ij} \pmod{p^e}$, this latter congruence and so also (4.6) has p_{ij} solutions $\pmod{p^e}$. Thus the number of incongruent solutions X_1, Y_1 of (4.6) and so of the congruence in (4.5), is p^{t^2} times as great for $e = b + 1$ as for $e = b$. Since X_2 and Y_2 in (4.5) can be chosen arbitrarily $\pmod{p^e}$, the number of incongruent solutions X_0, Y_0 of (4.5) is $p^{t(2m-t)}$ times as great for $e = b + 1$ as for $e = b$. Therefore, corresponding to any given U_k, V_k as defined above, the number of incongruent solutions X, Y of (4.3), which is equal to the number of incongruent solutions U, V of (1.1) with $a = k + 1$ such that $U \equiv U_k, V \equiv V_k \pmod{p^{k-b}}$, is $p^{t(2m-t)}$ times as great as the number $n(U_k, V_k)$ of such U, V for $a = k$. Since this holds for all the residue classes $\pmod{p^{k-b}}$ of such solutions U_k, V_k , it follows that under the given hypothesis

$$(4.7) \quad N(A, B, k + 1) = p^{t(2m-b)} N(A, B, k).$$

Finally, if we multiply (4.7) by p to the $(k + 1)(t^2 - 2mt)$ power and simplify, we get (4.1).

We note that in view of (4.7), Theorem 3 is equivalent to equation (3.3) under weaker hypotheses on A and B than those assumed in Theorem 2. Thus, taking A and B nonsingular $\pmod{p}$ in Theorem 3 and then using (4.7) along with (3.2) as before, we again get (3.1).

REFERENCES

- [1] J. H. HODGES, *Representations by bilinear forms in a finite field*, Duke Math. J. 22 (1955), 497-510.
 - [2] J. H. HODGES, *Some matrix equations over a finite field*, Annali di Matematica (IV) 44 (1957), 245-250.
 - [3] G. LANDSBERG, *Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, J. reine. angew. Math. 111 (1893), 87-88.
 - [4] C. C. MACDUFFEE, *The Theory of Matrices*, New York, 1946.
 - [5] C. L. SIEGEL, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. (2) 36 (1935), 527-606.
-