ACTA ARITHMETICA
XIX (1971)

# Gauss sums and the matrix equation $XX^T = 0$ over fields of characteristic two*

by

JOHN C. PERKINS (Clemson, South Carolina)

**1. Introduction.** Let $F_q$ denote the finite field of order $q = p^w$, $p$ a prime. Let $A$ and $B$ be symmetric matrices of order $n$, rank $m$, and order $s$, rank $k$, respectively, over $F_q$. Carlitz [2] has determined the number $N_s(A, B)$ of solutions $X$ over $F_q$, for $p$ an odd prime, to the matrix equation

$$XAX^T = B \tag{1.1}$$

of arbitrary rank when $n = m$. Furthermore, Hodges [7] has determined the number $N(A, B, r)$ of $s \times n$ matrices $X$ of rank $r$ over $F_q$, $p$ an odd prime, which satisfy (1.1).

One difficulty encountered in attempting to enumerate the solutions to (1.1) over a finite field $F_q$, where $q = 2^w$, is the fact that if $A$ is non-singular symmetric, then $A$ is not necessarily congruent to a diagonal matrix. In fact, if $A$ is symmetric with zero diagonal, then $A$ is congruent to the matrix

$$\begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}.$$

The purpose of this paper is to determine by means of Gauss sums the number $N_s(I, 0)$ of solutions $X$ over $F_q$, $q = 2^w$, of the matrix equation $XX^T = 0$, which is a special case of (1.1) with $A = I_n$ and $B = 0$. $N_s(I, 0)$ is given by Theorem 4.2.

In another paper [8], the author has enumerated the $s \times n$ matrices $X$ of given rank $r$ over $F_q$, $q = 2^w$, such that $XX^T = 0$.

In finding $N_s(I, 0)$, we use a method similar to that used by Carlitz to determine $N_s(A, B)$, and which employs Gauss sums over finite fields

---

* This paper is essentially Chapter 4, Section 1 of my doctoral dissertation under direction of John D. Fulton and submitted to the graduate faculty of Clemson University.

of order $q = 2^w$, also used by Carlitz [3]. The Gauss sums over $F_q$, $q = 2^w$, involve use of quadratic forms over $F_q$ dealt with in Section 2. Throughout this paper, unless otherwise specified, $K$ denotes a field of characteristic 2, while $F_q$ denotes a finite field of order $q = 2^w$. $V_n(K)$ denotes an $n$-dimensional vector space over $K$.

**2. Quadratic forms on $V_n(K)$.** In this section, we develop some of the theory of quadratic forms defined on fields of characteristic two necessary for the understanding of the application of Gauss sums to the matrix equation $XX^T = 0$ over $F_q$. For a classical treatment of this theory, the reader should examine the text by Chevalley [4].

A quadratic form on $V_n(K)$ is a function $Q$ from $V_n(K)$ into $K$ with the properties:

(2.1) $$Q(\lambda x) = \lambda^2 Q(x) \quad \text{for} \quad \lambda \in K,\ x \in V_n(K),$$

and

(2.2) the mapping $g$ from $V_n(K)\times V_n(K)$ into $K$ defined by

$$g(x, y) = Q(x+y)+Q(x)+Q(y), \quad (x, y) \in V_n(K)\times V_n(K)$$

is a bilinear form on $V_n(K)\times V_n(K)$.

It is clear from the above definition that the bilinear form $g$ is symmetric; that is, $g(x, y) = g(y, x)$ for all $x, y$ in $V_n(K)$. Moreover, $g(x, x) = Q(x+x)+Q(x)+Q(x) = 0$, and $g$ is alternating.

Let $Q$ be a quadratic form defined on $V_n(K)$ with associated bilinear form $g$. Let $\mathscr{B} = (u_1, \ldots, u_n)$ be a basis for $V_n(K)$. By extending properties (2.1) and (2.2) through induction and by writing $\xi = (\xi_1, \ldots, \xi_n)$ for $\xi = \xi_1 u_1 + \ldots + \xi_n u_n$, we obtain the expression

(2.3) $$Q(\xi) = \sum_{i=1}^{n} \xi_i^2 Q(u_i) + \sum_{1\leqslant i<j\leqslant n} \xi_i \xi_j g(u_i, u_j).$$

However, if $\mathscr{B}$ is properly chosen, the expression (2.3) for $Q$ takes a particularly simple form.

Dickson ([5], § 199) implies that a special basis can be chosen for $V_n(F_q)$. This basis gives Dickson's canonical forms, which can be found in the following theorem.

THEOREM 2.1. *If $Q$ is a quadratic form of rank $n$ on $V_n(F_q)$, there is a basis relative to which $Q$ takes one and only one of the following forms*:

(2.4) $$Q(\xi) = \xi_1\xi_{\nu+1}+\xi_2\xi_{\nu+2}+\ldots+\xi_\nu\xi_{2\nu}+\xi_{2\nu+1}^2 \quad (n = 2\nu+1),$$

(2.5) $$Q(\xi) = \xi_1\xi_{\nu+1}+\xi_2\xi_{\nu+2}+\ldots+\xi_\nu\xi_{2\nu} \quad (n = 2\nu), \quad \text{or}$$

(2.6) $$Q(\xi) = \xi_1\xi_{\nu+1}+\xi_2\xi_{\nu+2}+\ldots+\xi_{\nu-1}\xi_{2\nu-1}+\xi_\nu^2+\xi_\nu\xi_{2\nu}+\beta\xi_{2\nu}^2 \quad (n = 2\nu).$$



In (2.6), $\beta$ is any element of $F_q$ such that the polynomial $x^2+x+\beta$ is irreducible over $F_q$.

We can also obtain a corresponding theorem for quadratic forms of rank $r \leqslant n$.

THEOREM 2.2. *Let $Q$ be a quadratic form on $V_n(F_q)$ of rank $r \leqslant n$. Then there is a basis relative to which $Q$ takes one and only one of the following forms*:

(2.7) $$Q(\xi) = \xi_1\xi_{p+1}+\xi_2\xi_{p+2}+\ldots+\xi_p\xi_{2p+1}+\xi_{2p+1}^2 \quad (r = 2p+1),$$

(2.8) $$Q(\xi) = \xi_1\xi_{p+1}+\xi_2\xi_{p+2}+\ldots+\xi_p\xi_{2p} \quad (r = 2p), \quad \text{or}$$

(2.9) $$Q(\xi) = \xi_1\xi_{p+1}+\xi_2\xi_{p+2}+\ldots+\xi_{p-1}\xi_{2p-1}+\xi_p^2+\xi_p\xi_{2p}+\beta\xi_{2p}^2 \quad (r = 2p).$$

In (2.9), $\beta$ is any element of $F_q$ such that the polynomial $x^2+x+\beta$ is irreducible over $F_q$. Henceforth, for $n$ even, we shall say that $Q$ is of type $\tau = 1$ or $-1$ according as $Q$ has the form (2.5) or (2.6), respectively.

In (2.3), let

$$Q(u_i) = a_{ii} \quad (1 \leqslant i \leqslant n), \quad g(u_i, u_j) = a_{ij} \quad (1 \leqslant i < j \leqslant n).$$

The expression (2.3) for $Q$ relative to the basis $\mathscr{B}$ becomes

(2.10) $$Q(\xi) = \sum_{1\leqslant i\leqslant j\leqslant n} \xi_i \xi_j a_{ij}.$$

This is not the only expression which may be written for $Q$ relative to the basis $\mathscr{B}$. It is true, however, that (2.10) is the unique expression for $Q$ relative to $\mathscr{B}$, where the sum is over all $i, j$, such that $1 \leqslant i \leqslant j \leqslant n$. Consequently, (2.10) suggests that we associate with $Q$ a unique upper triangular matrix $A = [a_{ij}]$, with $a_{ij} = 0$, $1 \leqslant j < i \leqslant n$. Clearly, $Q(\xi) = \xi A \xi^T$, and we say that $A$ is the *matrix of $Q$ relative to the basis $\mathscr{B}$*. Furthermore, if $C$ is any upper triangular matrix over $K$, then relative to some basis the function on $V_n(K)$ defined by $Q(\xi) = \xi C \xi^T$ is a quadratic form on $V_n(K)$.

A symmetric matrix with zero diagonal is called an *alternate* matrix. Albert ([1], p. 397) has proved the following

THEOREM 2.3. *Let $Q_1$ and $Q_2$ be quadratic forms on $V_n(K)$ with matrices $A_1$ and $A_2$, respectively, where $A_1$ and $A_2$ are not necessarily upper triangular. Then $Q_1 = Q_2$ if and only if $A_1+A_2 = N$, where $N$ is an alternate matrix.*

The next theorem follows directly from Theorem 2.2.

THEOREM 2.4. *If $Q$ is a quadratic form of rank $r \leqslant n$ on $V_n(F_q)$, then there is a basis for $V_n(F_q)$ such that the matrix of $Q$ relative to this basis is*

$$\begin{bmatrix} G_{2\nu+\delta} & 0 \\ 0 & 0 \end{bmatrix},$$

*where* $2\nu+\delta = r$, $G_{2\nu+\delta}$ *is* $(2\nu+\delta)\times(2\nu+\delta)$ *and is one of the following*:

$$G_{2\nu+1} = \begin{bmatrix} 0 & I_\nu & \\ & 0 & \\ & & 1 \end{bmatrix}, \tag{2.11}$$

$$G_{2\nu} = \begin{bmatrix} 0 & I_\nu \\ & 0 \end{bmatrix}, \text{ or} \tag{2.12}$$

$$G_{2\nu+2} = \begin{bmatrix} 0 & I_\nu & & \\ & 0 & & \\ & & 1 & 1 \\ & & & \beta \end{bmatrix}. \tag{2.13}$$

Now let $\mathscr{B}_1$ and $\mathscr{B}_2$ be two bases for $V_n(K)$. Let $Q$ be a quadratic form on $V_n(K)$, and let $P$ be the $n\times n$ non-singular matrix relating the two bases. We now prove a theorem first proved by Albert ([1], p. 398).

THEOREM 2.5. *Let* $Q$ *have matrix* $A$ *relative to the basis* $\mathscr{B}_1$. *Then the matrix of* $Q$ *relative to* $\mathscr{B}_2$ *is* $D = PAP^T + N(A, P)$, *where* $N(A, P)$ *denotes the unique alternate matrix such that* $D$ *is an upper triangular matrix.*

Proof. Now $Q(\xi) = \xi A \xi^T$. Thus, if $\xi = \eta P$, then $Q(n) = \eta PAP^T\eta^T$. Hence, if $D$ is the matrix of $Q$ relative to $\mathscr{B}_2$, by Theorem 2.3, $D = PAP^T + N(A, P)$, where $N(A, P)$ is an alternate matrix.

If $A_1$ and $A_2$ are upper triangular matrices over $K$, we say that $A_1$ is *congruent to* $A_2$ if $A_1 = PA_2P^T + N(A_2, P)$, for some non-singular matrix $P$ and some unique alternate matrix $N(A_2, P)$. Let $A$ be an $n\times n$ matrix over $K$, where $A$ is not necessarily upper triangular. We say that $A$ is of rank $r$ if the quadratic form defined by $A$ is of rank $r$. Notice from (2.11), (2.12), or (2.13) that this is not the usual concept of rank of a matrix. The next theorem follows directly from Theorem 2.4 and Theorem 2.5.

THEOREM 2.6. *If* $A$ *is an upper triangular matrix of rank* $r$ *over* $F_q$, *then* $A$ *is congruent to a matrix*

$$F_r = \begin{bmatrix} G_r & 0 \\ 0 & 0 \end{bmatrix},$$

*where* $r = 2\nu+\delta$, $\delta = 0, 1, 2$, $G_r$ *is* $r\times r$ *and is given by* (2.11) *if* $\delta = 1$, (2.12) *if* $\delta = 0$, *and* (2.13) *if* $\delta = 2$.

The set of all non-singular matrices $P$ such that $PF_rP^T + N(F_r, P) = F_r$ forms a group. We calculate the order of this group in the next section. The set of all $P$ over $F_q$ such that

$$PG_{2\nu+\delta}P^T + N(G_{2\nu+\delta}, P) = G_{2\nu+\delta} \quad (\delta = 0, 1, 2),$$

is called the *orthogonal group associated with* $G_{2\nu+\delta}$, and is denoted by $O_{2\nu+\delta}$. Dickson ([5], § 115, § 204) has calculated the orders of $O_{2\nu+\delta}$, $\delta = 0, 1, 2$.



These are given as follows:

$$|O_{2\nu+1}| = (q^{2\nu}-1)q^{2\nu-1}(q^{2\nu-2}-1)q^{2\nu-3}\dots(q^2-1)q, \tag{2.14}$$

$$|O_{2\nu}| = 2(q^\nu-1)(q^{2(\nu-1)}-1)q^{2(\nu-1)}(q^{2(\nu-2)}-1)q^{2(\nu-2)}\dots(q^2-1)q^2, \tag{2.15}$$

$$|O_{2\nu+2}| = 2(q^\nu-1)(q^{2(\nu-2)}-1)q^{2(\nu-1)}(q^{2(\nu-2)}-1)q^{2(\nu-2)}\dots(q^2-1)q^2, \tag{2.16}$$

where $q = 2^w$.

The next theorem will be used in Section 4.

THEOREM 2.7. *Let* $F_r$ *be as in Theorem* 2.6. *For* $P$ *and* $R$ *non-singular matrices,*

$$PF_rP^T + N(F_r, P) = RF_rR^T + N(F_r, R)$$

*if and only if there is a non-singular matrix* $B$ *such that* $P = RB$, *where* $BF_rB^T + N(F_r, B) = F_r$.

Proof. Suppose $PF_rP^T + N(F_r, P) = RF_rR^T + N(F_r, R)$. Then

$$R^{-1}PF_rP^T(R^{-1})^T + R^{-1}N(F_r, P)(R^{-1})^T = F_r + R^{-1}N(F_r, R)(R^{-1})^T. \tag{2.17}$$

If we let $B = R^{-1}P$, and $N(F_r, B) = R^{-1}\big(N(F_r, P) + N(F_r, R)\big)(R^{-1})^T$, then $N(F_r, B)$ is alternate and (2.17) becomes $BF_rB^T + N(F_r, B) = F_r$.

If there is a $B$ such that $P = RB$ and $BF_rB^T + N(F_r, B) = F_r$, then

$$R^{-1}PF_rP^T(R^{-1})^T + N(F_r, B) = F_r.$$

Thus,

$$PF_rP^T + RN(F_r, B)R^T = RF_rR^T. \tag{2.18}$$

Let $N(F_r, P)$ be an alternate matrix such that $PF_rP^T + N(F_r, P)$ is upper triangular. Then (2.18) becomes

$$PF_rP^T + N(F_r, P) = RF_rR^T + N(F_r, P) + RN(F_r, B)R^T.$$

The matrix $N(F_r, R) = N(F_r, P) + RN(F_r, B)R^T$ must be the unique alternate matrix such that $RF_rR^T + N(F_r, R)$ is upper triangular.

**3. Gauss sums over** $F_q$. For $a \in F_q$, $q = 2^w$, let $t$ be a mapping from $F_q$ to $F_q$ defined by

$$t(a) = a + a^2 + \dots + a^{2^{R-1}}.$$

Then $t$ is a mapping from $F_q$ onto the prime subfield of $F_q$; that is, for each $a \in F_q$, $t(a) = m\cdot 1$, $m = 0, 1$. Here 1 denotes the multiplicative identity in $F_q$. Also, $t(a+\beta) = t(a) + t(\beta)$ for $\alpha, \beta$, in $F_q$.

Define a mapping $e$ from $F_q$ to the multiplicative subgroup $\{1, -1\}$ of the reals by

$$e(a) = (-1)^m, \tag{3.1}$$

where $t(a) = m \cdot 1$. It is easily seen that $e(\alpha+\beta) = e(\alpha)e(\beta)$ for all $\alpha, \beta$ in $F_q$. The function (3.1) also satisfies

$$\sum_{r \in F_q} e(\alpha r) = \begin{cases} q & (\alpha = 0), \\ 0 & (\alpha \neq 0). \end{cases} \tag{3.2}$$

Let $Q$ be a quadratic form on $V_n(F_q)$, and let $(x_1, \ldots, x_n)$ be a basis for $V_n(F_q)$, so that if $\xi = \xi_1 x_1 + \ldots + \xi_n x_n$, then relative to this basis

$$Q(\xi) = \sum_{1 \leqslant i \leqslant j \leqslant n} \xi_i \xi_j b_{ij}.$$

Define

$$S(Q) = \sum_{\xi \in V_n(F_q)} e\big(Q(\xi)\big),$$

where the sum is over all $\xi = \xi_1 x_1 + \ldots + \xi_n x_n$ in $V_n(F_q)$. Write $\xi$ as $(\xi_1, \ldots, \xi_n)$. We note that if $P$ is an $n \times n$ non-singular matrix over $F_q$,

$$\sum_{\xi \in V_n(F_q)} e\big(Q(\xi P)\big) = \sum_{\xi \in V_n(F_q)} e\big(Q(\xi)\big). \tag{3.3}$$

Suppose quadratic forms $Q_1$ and $Q_2$ are such that $Q_1(\xi) = Q_2(\xi P)$, $\xi \in V_n(F_q)$. Therefore, by (3.3), $S(Q_1) = S(Q_2)$. Consequently, in the evaluation of $S(Q)$, $Q$ may be assumed to be in one of the canonical forms (2.7), (2.8) or (2.9). In the next two theorems, Carlitz [3] has shown how $S(Q)$ may be evaluated.

THEOREM 3.1. *Let*

$$Q(\xi) = \sum_{1 \leqslant i \leqslant j \leqslant n} \xi_i \xi_j b_{ij} \qquad (b_{ij} \in F_q)$$

*be a quadratic form of rank $n$ on $V_n(F_q)$. Then*

$$S(Q) = \begin{cases} 0 & (n \text{ odd}), \\ \tau q^{n/2} & (n \text{ even}), \end{cases}$$

*where $\tau$ denotes the type of $Q$.*

THEOREM 3.2. *Let*

$$Q(\xi) = \sum_{1 \leqslant i \leqslant j \leqslant n} \xi_i \xi_j b_{ij} \qquad (b_{ij} \in F_q)$$

*be a quadratic form on $V_n(F_q)$ of rank $r \leqslant n$. Then*

$$S(Q) = \begin{cases} 0 & (r \text{ odd}), \\ \tau q^{(2n-r)/2} & (r \text{ even}). \end{cases}$$



**4. The determination of $N_s(I, 0)$.** Let $A = [a_{ij}]$ be an $s \times s$ symmetric matrix over $F_q$, and denote the trace of an $n \times n$ matrix $E$ by $\sigma(E)$.

It follows from (3.2) that

$$\sum_{B} e\big(\sigma(AB)\big) = \begin{cases} q^{s(s+1)/2} & (A = 0), \\ 0 & (A \neq 0), \end{cases} \tag{4.1}$$

where $A$ is symmetric and where the sum is over all $s \times s$ upper triangular matrices $B$. For every $X$, $XX^T$ is symmetric, and from (4.1)

$$q^{s(s+1)/2} N_s(I, 0) = \sum_{B} \sum_{X} e\big(\sigma(XX^T B)\big),$$

where the first sum is over all $s \times s$ upper triangular matrices $B$, and the second sum is over all $s \times n$ matrices $X$. Let $B = [b_{ij}]$, $A = [a_{ij}]$ and $X = [x_{ij}]$. Then

$$\sigma(XX^T B) = \sum_{k=1}^{n} \sum_{j=1}^{s} \sum_{i=1}^{s} x_{ik} x_{jk} b_{ji}. \tag{4.2}$$

Let $x_k = (x_{1k}, \ldots, x_{sk})$. By using the notation $B(x_k) = x_k B x_k^T$, we may write (4.2) as

$$\sigma(XX^T B) = \sum_{k=1}^{n} B(x_k).$$

Each upper triangular matrix $B$ defines some quadratic form $Q_B$. Let $S(Q_B) = S(B)$. Write $r(B)$ for the rank of $B$. By using the properties of $e$, (4.1) becomes

$$\begin{aligned} q^{s(s+1)/2} N_s(I, 0) &= \sum_{B} \sum_{X} \prod_{k=1}^{n} e\big(B(x_k)\big) \\ &= \sum_{B} [s(B)]^n = \sum_{\substack{B \\ r(B) \text{ odd}}} [s(B)]^n + \sum_{\substack{B \\ r(B) \text{ even}}} [s(B)]^n. \end{aligned} \tag{4.3}$$

But if the rank of $B$ is odd, by Theorem 3.2, $S(B) = 0$, and $S(B) = \tau q^{(2s-r)/2}$ for $B$ of even rank $r$, where $\tau = \pm 1$ depending on the type of quadratic form defined by $B$. In fact, $\tau = 1$ if $B$ is congruent to

$$\begin{bmatrix} G_{2\nu} & 0 \\ 0 & 0 \end{bmatrix}, \qquad r = 2\nu,$$

and $\tau = -1$ if $B$ is congruent to

$$\begin{bmatrix} G_{2\nu+2} & 0 \\ 0 & 0 \end{bmatrix}, \qquad r = 2\nu+2,$$

where $G_{2\nu}$ is given by (2.12) and $G_{2\nu+2}$ is given by (2.13). Let $n(s, r, \tau)$ be the number of $s \times s$ upper triangular matrices $B$ of rank $r$ and type $\tau$. We may then write

$$q^{s(s+1)/2} N_s(I, 0) = \sum_{\substack{r=0 \\ r \text{ even}}}^{s} n(s, r, 1)\,(q^{(2s-r)/2})^n + (-1)^n \sum_{\substack{r=2 \\ r \text{ even}}}^{s} n(s, r, -1)\,(q^{(2s-r)/2})^n.$$

Since every upper triangular matrix $B$ of rank $r = 2\nu+\delta$, $\delta = 0, 1, 2$ is congruent to some unique upper triangular $F_r$, where $F_r$ is in canonical form, $n(s, r, \tau)$ is just the number of matrices $B$ each of which has canonical form

$$F_r = \begin{bmatrix} G_r & 0 \\ 0 & 0 \end{bmatrix}, \tag{4.4}$$

where $G_r$ is given by (2.12) if $r = 2\nu$ and by (2.13) if $r = 2\nu+2$.

If we take a particular $F_r$ of the form (4.4) and apply all $s \times s$ non-singular matrices $P$, $PF_rP^T + N(F_r, P)$ will give all $s \times s$ upper triangular matrices of rank $r$ and type $\tau$. However, duplications may arise in this process. We now account for these duplications.

By Theorem 2.7, we must count the number of $B$'s such that $BF_rB^T + N(F_r, B) = F_r$. We proceed as in [6]. Let this number be $\varrho(s, r, \tau)$ with $r = 2\nu$ or $r = 2\nu+2$, and let

$$B = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix},$$

where $B_1$ is $(2\nu+\delta) \times (2\nu+\delta)$, $B_2$ is $(2\nu+\delta) \times (s-(2\nu+\delta))$, $B_3$ is $(s-(2\nu+\delta)) \times (2\nu+\delta)$, and $B_4$ is $(s-(2\nu+\delta)) \times (s-(2\nu+\delta))$. Then

$$BF_rB^T + N(F_r, B) = \begin{bmatrix} B_1G_rB_1^T + N(G_r, B_1) & B_1(G_r+G_r^T)B_3^T \\ 0 & B_3G_rB_3^T + N(G_r, B_3) \end{bmatrix}, \tag{4.5}$$

If $F_r$ is given by (4.4), then by (4.5)

$$B_1G_rB_1^T + N(G_r, B_1) = G_r, \tag{4.6}$$

$$B_1(G_r+G_r^T)B_3^T = 0, \tag{4.7}$$

and

$$B_3G_rB_3^T + N(G_r, B_3) = 0. \tag{4.8}$$

By (4.6), $B_1$ must be in the orthogonal group $O_{2\nu+\delta}$ relative to the matrix $G_r = G_{2\nu+\delta}$. Therefore, the number of ways to choose $B_1$ is known. To



determine the number of ways to choose $B_2$, $B_3$, and $B_4$, we treat the cases $r = 2\nu+\delta$, $\delta = 0, 2$, separately. Suppose $r = 2\nu+2$. Then

$$G_r + G_r^T = \begin{bmatrix} 0 & I_\nu & & \\ I_\nu & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix}.$$

Consequently, $G_r + G_r^T$ is non-singular, and since $B_1$ is non-singular, $B_4$ must be non-singular. The matrix $B_2$ is arbitrary. The number of ways to choose $B_4$ is $g(s-2\nu-2)$, where

$$g(k) = \prod_{i=1}^{k} (q^k - q^{i-1}), \tag{4.9}$$

and the number of ways to choose $B_2$ is $q^{(2\nu+2)(s-2\nu-2)}$. Therefore,

$$\varrho(s, 2\nu+2, -1) = |O_{2\nu+2}|\, g(s-2\nu-2)\, q^{(2\nu+2)(s-2\nu-2)}, \tag{4.10}$$

where $|O_{2\nu+2}|$ is given by (2.16).

The number $\varrho(s, 2\nu, 1)$ is calculated in a similar manner, and

$$\varrho(s, 2\nu, 1) = |O_{2\nu}|\, g(s-2\nu)\, q^{(2\nu)(s-2\nu)}, \tag{4.11}$$

where $|O_{2\nu}|$ is given by (2.15).

Define a relation $\sim$ on $\mathrm{GL}(s, q)$, the set of all $s \times s$ non-singular matrices over $F_q$, as follows: $P \sim P'$ if and only if there is a $B$ such that $BF_rB^T + N(F_r, B) = F_r$ and such that $P = P'B$. It is easily verified that $\sim$ is an equivalence relation on $\mathrm{GL}(s, q)$. Thus, $\sim$ induces a partitioning of $\mathrm{GL}(s, q)$, the sets of the partition being the equivalence classes under $\sim$. Each equivalence class contains the same number of elements, namely, $\varrho(s, 2\nu+\delta, \tau)$ elements. If $\mathscr{P}$ is a set composed of one element from each equivalence class, then the order of $\mathscr{P}$ is just the number we seek; that is,

$$n(s, 2\nu+\delta, \tau) = \frac{g(s)}{\varrho(s, 2\nu+\delta, \tau)}.$$

We have proved the following theorem.

THEOREM 4.1. *The number of matrices $PF_rP^T + N(F_r, P)$ as $P$ ranges through $\mathrm{GL}(s, q)$, where $F_r$ is given by* (4.4), *is*

$$n(s, 2\nu+2, -1) = \frac{g(s)}{\varrho(s, 2\nu+2, -1)},$$

*or*

$$n(s, 2\nu, 1) = \frac{g(s)}{\varrho(s, 2\nu, 1)},$$

*where* $\varrho(s, 2v+2, -1)$ *is given by* (4.10), $\varrho(s, 2v, 1)$ *is given by* (4.11), *and* $g(s)$ *is given by* (4.9).

Hence, we have proved the following

THEOREM 4.2. *The number of* $s \times n$ *matrices* $X$ *over* $F_q$ *such that* $XX^T = 0$ *is*

$$N_s(I, 0) = \frac{1}{q^{s(s+1)/2}} \left\{ \sum_{\substack{r=0 \\ r \text{ even}}}^{s} \frac{g(s)}{\varrho(s, r, 1)} (q^{(2s-r)/2})^n + \sum_{\substack{r=1 \\ r \text{ odd}}}^{s} \frac{g(s)}{\varrho(s, r, -1)} (q^{(2s-r)/2})^n \right\}.$$

**References**


[1] A. A. Albert, *Symmetric and alternate matrices in an arbitrary field, I*, AMS Trans. 43 (1938), pp. 386–436.

[2] L. Carlitz, *Representations by quadratic forms in a finite field*, Duke Math. J. 21 (1954), pp. 123–137.

[3] — *Gauss sums over finite fields of order* $2^n$, Acta Arith. 15 (1969), pp. 247–267.

[4] C. Chevalley, *The Algebraic Theory of Spinors*, New York 1954.

[5] L. E. Dickson, *Linear Groups With an Exposition of the Galois Theory*, Leipzig: Reprinted by Dover, 1958.

[6] Xu-ning Feng (Hsii-ning Feng) and Zong-duo Dai (Tsung-tuo Tai), *Studies in finite geometries and the construction of incomplete block designs V, Some Anzahl theorems in orthogonal geometry over finite fields of characteristic* 2, Chinese Math. Acta. 15 (1965), pp. 392–410.

[7] John H. Hodges, *A symmetric matrix equation over a finite field*, Math. Nachr. 30 (1965), pp. 221–228.

[8] John C. Perkins, *Rank r solutions to the matrix equation* $XX^T = 0$ *over a field of characteristic* 2, Math. Nachr. (to appear).


*Received on 8. 3. 1970* 56

ACTA ARITHMETICA
XIX (1971)

# On a problem of Schinzel concerning principal divisors in arithmetic progressions

by

CHARLES J. PARRY (East Lansing, Mich.)

The following problem was proposed by A. Schinzel at the A. M. S. Number Theory Institute held at Stony Brook, New York in July of 1969.

QUESTION I. *Let* $f(x)$ *be a primitive polynomial and* $k$ *an algebraic number field. Do there exist infinitely many integers* $x$ *such that* $f(x)$ *factors into principal ideals in* $k$? (*unknown even for* $f$ *linear*).

For the case that $f$ is linear, I prove here that the answer is yes. It has been noted [2] for polynomials of higher degree that the following additional assumptions are necessary:

(i) the content of any factor of $f(x)$ in $k$ is principal (MacCluer);
(ii) each fixed divisor of $f(x)$ is principal (Schinzel).

**Introduction.** In the linear case, that is, when $f(x) = mx+b$ with $(m, b) = 1$, it seems reasonable to ask the slightly stronger:

QUESTION II. *Do there exist infinitely many primes of the form* $mx+b$ *which split into principal prime ideals in* $k$?

The following example (MacCluer) shows that the answer to Question II is no. (Schinzel has informed me that a similar counterexample was found earlier by J. Tate.)

The number field $Q(\sqrt{10})$ has class number $h = 2$ and Hilbert class field $\mathrm{CF}(Q(\sqrt{10})) = Q(\sqrt{2}, \sqrt{5})$. According to Artin reciprocity, a rational prime $p \neq 2, 5$ has non-principal divisors in $Q(\sqrt{10})$ when and only when $p$ splits in $Q(\sqrt{10})$ into two distinct prime divisors, each of which remains prime in $Q(\sqrt{2}, \sqrt{5})$, in Legendre symbols this is equivalent to

$$\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = -1$$

which obtains when and only when $p \equiv \pm 3, \pm 13 \pmod{40}$. Thus for instance, no prime of the form $p = 40x+3$ has principal divisors in $Q(\sqrt{10})$.