Internat. J. Math. & Math. Sci.
VOL. 16 NO. 3 (1993) 539-544

ON THE MATRIX EQUATION $X^n = B$ OVER FINITE FIELDS

MARIA T. ACOSTA-DE-OROZCO and JAVIER GOMEZ-CALDERON

Department of Mathematics
Southwest Texas State University
San Marcos, Texas 78666-4603

Department of Mathematics
The Pennsylvania State University
New Kensington Campus
New Kensington, Pennsylvania 15068

(Received May 28, 1992 and in revised form April 19, 1993)

ABSTRACT. Let $GF(q)$ denote the finite field of order $q = p^e$ with p odd and prime. Let M denote the ring of $m \times m$ matrices with entries in $GF(q)$. In this paper, we consider the problem of determining the number $N = N(n, m, B)$ of the n-th roots in M of a given matrix $B \in M$.

KEY WORDS AND PHRASES. Finite fields and matrix powers.
1991 AMS SUBJECT CLASSIFICATION CODE. 15A33.

1. INTRODUCTION.

Let $GF(q)$ denote the finite field of order $q = p^e$ with p odd and prime. Let $M = M_{m \times m}(q)$ denote the ring of $m \times m$ matrices with entries in $GF(q)$. In this paper, we consider the problem of determining the number $N = N(n, m, B)$ of the n-th roots in M of a given matrix $B \in M$; i.e., the number of solutions X in M of the equation

$$x^n = B \tag{1.1}$$

Our present work generalizes a recent paper of the authors [1] in which the case $N(n, 2, B)$ was considered. If B denotes a scalar matrix, then equation (1.1) is called *scalar equation*, type of equations that has been already studied by Hodges in [3]. Also, if B denotes the identity matrix and $n = 2$, then the solutions of (1.1) are called *involutory matrices*. Involutory matrices over either a finite field or a quotient ring of the rational integers have been extensively researched, with a detailed extension to all finite commutative rings given by McDonald in [5].

2. ESTIMATING $N(n, m, B)$.

Let $GF(q)$ denote the finite field of order $q = p^e$ with p odd and prime. Let $M = M_{m \times m}(q)$ denote the ring of $m \times m$ matrices with entries in $GF(q)$ and let $GL(q, m)$ denote its group of units. We now make the following conventions:

(a) n and m will denote integers so that $1 < m$ and $1 < n < q$,

(b) $N(n, m, B)$ will denote the number of solutions X in M of the equation

$$X^n = B$$

(c) $g(m, d)$ will denote the cardinality of $GL(q^d, m)$. Thus

$$g(m, d) = \prod_{i=o}^{m-1} (q^{md} - q^{id})$$

$$= q^{dm^2} \prod_{i=1}^{m} (1 - q^{-id})$$

We also define $g(0, d) = 1$.

Our first lemma is a result given by Hodges in ([3], Th. 2).

LEMMA 1. Suppose $E(x)$ is a monic polynomial over $GF(q)$ with factorization given by

$$E(x) = F_1^{h_1} F_2^{h_2} \cdots F_s^{h_s}$$

where the F_i are distinct monic irreducible polynomials, $h_i \geq 1$ and $degF_i = d_i$ for $i = 1, 2, \cdots, s$. Then the number of matrices B in M such that $E(B) = 0$ is given by

$$g(m,1)\sum_P q^{-a(P)} \prod_{i=1}^{s} \prod_{j=1}^{h_i} g(K_{ij}, d_i)^{-1}$$

where the summation is over all partitions $P = P(m)$ defined by

$$m = \sum_{i=1}^{s} d_i \sum_{j=1}^{h_i} jk_{ij},\ k_{ij} \geq O$$

and $a(P) = \sum_{i=1}^{s} d_i b_i(P)$ where $b_i(P)$ is defined by

$$b_i(P) = \sum_{u=1}^{h_i} \left[k_{iu}^2 (u-1) + 2u\, k_{iu} \sum_{v=u+1}^{h_i} k_{iv} \right]$$

LEMMA 2. Let w denote a primitive element of $GF(q)$. Let $r \in GF(q)* = GF(q) - \{0\}$ and write $r = w^t$ for some t, $1 \leq t \leq q-1$. Assume n divides $q-1$ but 4 is not factor of n. Then

$$\sum_P q^m (q-1)^m \leq N(n,m,rl) \leq \sum_P \frac{q^{m^2}}{(q-1)^m}$$

where the summation is over all partitions $P = P(m)$ defined by

$$m = \frac{n}{(n,t)} \sum_{i=1}^{(n,t)} k_i,\quad k_i \geq 0$$

PROOF. Let D denote the greatest common divisor of n and t. Then

$$\begin{aligned} x^n - w^t &= \left(x^{\frac{n}{D}}\right)^D - \left(w^{\frac{t}{D}}\right)^D \\ &= \prod_{i=0}^{D-1} \left(x^{\frac{n}{D}} - w^{\frac{(q-1)}{D} i + \frac{t}{D}} \right) \\ &= \prod_{i=0}^{D-1} h_i(x). \end{aligned}$$

We also see that $w^{\frac{(q-1)}{D} i + \frac{1}{D}}$ does not belong to the set of powers $GF^S(q) = \{x^s : x \in GF(q)\}$ for all prime factors s of $\frac{n}{D}$. Hence, by ([4], Ch. VIII, Th. 16), each factor $h_i(x)$ is irreducible over $GF(q)[x]$. Therefore, Lemma 1 with $E(x) = x^n - w^t$ gives

$$N(n,m,r\ l) = g(m,1) \sum_P \prod_{i=1}^{D} g\left(k_i, \frac{n}{D}\right)^{-1} \tag{2.1}$$

where the summation over all partition $P = P(m)$ defined by

$$m = \frac{n}{D} \sum_{i=1}^{D} k_i, k_i \geq 0.$$

Hence,

$$N(n,m,r\ l) = \sum_P \frac{q^{m^2} \prod_{i=1}^{m} (1 - q^{-1})}{q^{\frac{n}{D} \sum_{i=1}^{n} k_i^2} \prod_{i=1}^{n} \prod_{j=1}^{k_i} (1 - q^{-\frac{n}{D} j})}$$

$$\leq \sum_P \frac{q^{m^2}}{q^m}\left(\frac{q}{q-1}\right)^m$$

$$= \sum_P \frac{q^{m^2}}{(q-1)^m}$$

and

$$N(n,m,rl) = \sum_P \frac{q^{m^2}\prod_{i=1}^{m}(1-q^{-1})}{q^{\frac{n}{D}\sum_{i=1}^{n} k_i^2}\prod_{i=1}^{n}\prod_{j=1}^{k_i}(1-q^{-\frac{n}{D^j}})}$$

$$\geq \sum_P \frac{q^{m^2}(1-q^{-1})^m}{q^{\frac{n}{D}\sum_{i=1}^{n} k_i^2}}$$

$$\geq \sum_P q^m(q-1)^m$$

REMARK 1. If $r^m = w^{tm} \notin GF^n(q)$, then n does not divide tm and the number of partitions P is zero. Thus, $N(n,m,rl) = 0$.

REMARK 2. If $r = w^{q-1} = 1$ and $1 < n < q$, including 4 as a possible factor of n, then one can obtain

$$\sum_P q^m \leq N(n,m,l) \leq \sum_P \frac{q^{m^2}}{(q-1)^m}$$

LEMMA 3. $$\sum_P (q-1)^m \leq N(n,m,0) \leq \sum_P \frac{q^{m^2}}{(q-1)^m}$$

where P denotes all partitions $P = P(m)$ defined by

$$m = \sum_{j=1}^{n} j\,k_j, \qquad k_j \geq 0$$

PROOF. Applying Lemma 1, with $E(x) = x^n$, we obtain

$$N(n,m,0) = g(m,1)\sum_P q^{-b(P)}\prod_{j=1}^{n} g(k_j,1)^{-1}$$

where the summation is over all partitions $P = P(m)$ defined by

$$m = \sum_{j=1}^{n} j\,k_j, \qquad k_j \geq 0$$

and $b(P) = \sum_{u=1}^{n}\left[k_u^2(u-1) + 2uk_u\sum_{v=u+1}^{n} k_v\right]$. Therefore,

(a) $$N(n,m,o) = \sum_P \frac{q^{m^2}\prod_{i=1}^{m}(1-q^{-i})}{q^{b(P)}q^{\sum_{i=1}^{m} k_i^2}\prod_{i=1}^{n}\prod_{j=1}^{k_i}(1-q^{-j})}$$

where

$$b(P) + \sum_{i=1}^{n} k_i^2 = \sum_{u=1}^{n}\left[k_{iu}(u-1) + 2uk_{iu}\sum_{v=u+1}^{n} k_{iv}\right] + \sum_{i=1}^{n} k_i^2 \geq m.$$

We also see that $\frac{1-q^{-i}}{1-q^{-1}} \leq \frac{q}{q-1}$. Thus,

$$N(n,m,0) \leq \sum_P \frac{q^{m^2}}{q^m}\left(\frac{q}{q-1}\right)^m = \sum_P \frac{q^{m^2}}{(q-1)^m}.$$

(b) $$N(n,m,o) = \sum_P \frac{q^{m^2}\prod_{i=1}^{m}(1-q^{-i})}{q^{b(P)}\, q^{\sum_{i=1}^{n} k_i^2} \prod_{i=1}^{n}\prod_{j=1}^{k_i}(1-q^{-j})}$$

$$\geq \sum_P \frac{q^{m^2}(1-q^{-1})^m}{q^{b(P)+\sum_{i=1}^{n} k_i^2}}$$

$$= \sum_P \frac{q^{m^2}(q-1)^m}{q^{b(P)+m+\sum_{i=1}^{n} k_i^2}}$$

$$\geq \sum_P (q-1)^m.$$

Now we will consider a nonscalar matrix B. We start with the following

LEMMA 4. Let B denote a $m \times m$ matrix over $GF(q)$ with a minimal polynomial $f_B(x)$. Let $f_B(x) = f_1^{b_1}(x) f_2^{b_2}(x) \cdots f_r^{b_r}(x)$ with $deg(f_i) = d_i$ denote the prime factorization of $f_B(x)$. Assume that B is similar to a matrix of the form

$$diag\ (\underbrace{C(f_1^{b_1}), \cdots, C(f_1^{b_1})}_{k_1} \cdots, \underbrace{C(f_r^{b_r}), \cdots, C(f_r^{b_r})}_{k_r})$$

where $C(f_i^{b_i})$ denotes the companion matrix of $f_i^{b_i}$.

Let $f_i(x^n) = \prod_{j=1}^{a_i} F_{i,j}(x)$ denote the prime factorization of $f_i(x^n)$ for $i = 1,2,\cdots,r$. Let D_i denote the degree of $F_{i,j}(x)$ for $j = 1,2,\cdots,a_i$. Then

$$N(n,b,B) \leq \sum_P \frac{\prod_{i=1}^{r} g(k_i,d_i)}{\prod_{i=1}^{r}\prod_{j=1}^{a_i} g(R_{ij},D_i)} \tag{2.2}$$

where the summation is over all partitions $P = P(a_i, D_i, d_i, k_i)$ defined by

$$D_i \sum_{j=1}^{a_i} R_{ij} = d_i\, k_i, \qquad R_{ij} \geq 0$$

for $i = 1,2,\cdots,r$.

PROOF. If $T^n = B$ then $f_B(T^n) = 0$. Thus the minimal polynomial of T divides $f_B(x^n)$ and T is similar to a matrix of the form

$$diag(E_1, E_2, \cdots, E_r) \tag{2.3}$$

where

$$E_i = diag(\underbrace{C(F_{i1}^{b_i}), \cdots, C(F_{i1}^{b_i})}_{R_{i1}}, \cdots, \underbrace{C(F_{ia_i}^{b_i}), \cdots, C(F_{ia_i}^{b_i})}_{R_{ia_i}})$$

with $C(F_{ij}^{b_i})$ denoting the companion matrix of $F_{ij}^{b_i}$. So, we have a partition $P = P(a_i, D_i, d_i, k_i)$ defined by

$$D_i \sum_{j=1}^{a_i} R_{ij} = d_i k_i \tag{2.4}$$

for $i = 1,2,\cdots,r$. Therefore,

$$N(n,m,B) \leq \sum_P \frac{|\,com(B)\,|}{|\,com(T)\,|}$$

where $com(H)) = \{X \in GL(q,m) : XH = HX\}$ and the summation is over all partitions P defined

by (2.4).

Now using the formula for $|COM(H)|$ given by L.E. Dickson in ([2], p. 235) we obtain

$$N(n,m,B) \leq \sum_{P} \frac{\prod_{\iota=1}^{r} g(k_\iota, d_\iota)}{\prod_{\iota=1}^{r} \prod_{j=1}^{a_\iota} g(R_{\iota j}, D_\iota)}$$

This completes the proof of the lemma.

REMARK. If T is similar to a matrix of the form given in (2.3), then T^n may have elementary divisors of the form $f_i^{C_\iota}(X)$ with $C_\iota < b_\iota$. This possibility is the main problem to get an equality at (2.2).

LEMMA 5. Let B denote a $m \times m$ matrix over $GF(q)$ with minimal polynomial $f_B(x)$. Let $f_B(x) = f_1^{b_1}(x) f_2^{b_2}(x) \cdots f_r^{b_r}(x)$ with $d_\iota = deg(f_\iota)$ denote the prime factorization of $f_B(x)$. Assume $m = \sum_{\iota=1}^{r} b_\iota d_\iota$. Then

$$N(n,m,B) \leq n^r \leq n^m$$

Further, $N(n,m,B) = n^m$ if and only if $f_\iota(x) = x - a_\iota$ with $a_\iota \in GF^n(q)$ for $i = 1,2,\cdots,r = m$.

PROOF. With notation as in Lemma 4, $m = \sum_{\iota=1}^{r} b_\iota d_\iota$ implies $k_\iota = k_2 = \cdots = k_r = 1$. Therefore, if $T^n = B$ then $D_\iota = d_\iota$ for all $\iota = 1,2,\cdots,r$ and

$$N(n,m,B) \leq \sum_{P} 1$$

where the summation is over all partitions P defined by

$$\sum_{j=1}^{a_\iota} R_{\iota j} = 1, \qquad R_{\iota j} \geq 0$$

for $i = 1,2,\cdots,r$. Thus,

$$N(n,m,B) \leq \prod_{i=1}^{r} a_\iota \geq n^r$$

Now if $N(n,m,B) = n^m$, then $r = m$. So, each polynomial $f_i^{b_\iota}(x)$ must be linear so that $f_\iota(x^n)$ splits as a product of n distinct linear factors. Hence, $f_\iota(x) = x - a_\iota$ with $a_\iota \in GF^n(q)$ for $i = 1,2,\cdots,r = m$. Conversely, if $f_\iota(x) = x - a_\iota$ with $a_\iota \in GF^n(q)$, then

$$Q^{-1}\, diag\,(e_1, e_2, \cdots, e_m)\, Q = B$$

for some matrix Q in $GL(q,m)$ and for all e_ι in $GF(q)$ such that $e_\iota^n = a_\iota$ for $i = 1,2,\cdots,r$. Therefore,

$$N(n,m,B) = n^m.$$

COROLLARY 6. If $B = diag(b_1, b_2, \cdots, b_m)$ with $b_\iota \neq b_j$ when $i \neq j$, then

$$N(n,m,B) = \begin{cases} n^m \text{ if } b_\iota \in GF^n(q) \text{ for } i = 1,2,\cdots,m \\ 0, \text{ otherwise} \end{cases}$$

LEMMA 7. Let B denote a $m \times m$ matrix over $GF(q)$. Assume that the minimal polynomial of B is irreducible of degree $d < m$. Then, either $N(n,m,B) = 0$ or $N(n,m,B) \geq (q^d - 1)^{m/d}$.

PROOF. Let $f_B(x)$ denote the minimal polynomial of a $m \times m$ matrix B over $GF(q)$. Assume $f_B(x)$ is irreducible of degree $d < m$. Thus, $m = rd$ for some integer $r \geq 2$. Let $f_B(x^n) = F_1(x) F_2(x) \cdots F_a(x)$ denote the prime factorization of $f_B(x^n)$ and let D denote the degree of each of the factors $F_\iota(x)$ for $i = 1,2,\cdots,a$. Assume $N(n,m,B) > 0$. Then $T^n = B$ for some matrix T that is similar to a matrix of the form

$$diag\,(\underbrace{C(F_1), \cdots, C(F_1)}_{R_1} \cdots, \underbrace{C(F_a), \cdots, C(F_a)}_{R_a})$$

where $C(F_i)$ denote the companion matrix of $F_i(x)$ for $i = 1,2,\cdots,a$.

Therefore,

$$N(n,m,B) \geq \frac{|COM(B)|}{|COM(T)|}$$

$$\geq \frac{q^{dr^2} \prod_{j=1}^{r} (1-q^{-d_j})}{q^{D\sum_{i=1}^{a} R_i^2} \prod_{i=1}^{a} \prod_{j=1}^{R_i} (1-q^{-D_j})}$$

$$\geq \frac{q^{dr^2}(1-q^{-d})^r}{q^{D\sum_{i=1}^{a} R_i^2}}$$

$$\geq \begin{cases} \dfrac{q^{m(r-1)}(q^d-1)^r}{q^{m(\frac{m}{D}-1)}} & \text{if } m > d \\ \dfrac{q^{m(r-1)}(q^d-1)^r}{q^m} & \text{if } m = D \end{cases}$$

$$\geq (q^d-1)^{m/d}.$$

We are ready for our final result.

THEOREM 8. Let B denote a $m \times m$ matrix over $GF(q)$ and let $f_B(x)$ denote its minimal polynomial. Let $f_B(x) = f_1^{b_1}(x)\, f_2^{b_2}(x) \cdots f_r^{b_r}(x)$ with $deg(f_i) = d_i$ denote the prime factorization of $f_B(x)$. Assume B is similar to a matrix of the form

$$diag\ (\underbrace{C(f_1^{b_1}),\cdots,C(f_1^{b_1})}_{k_1} \cdots, \underbrace{C(f_r^{b_r}),\cdots,C(f_r^{b_r})}_{k_r})$$

where $C(f_i^{b_i})$ denotes the companion matrix of $f_i^{b_i}$.

Let $f_i(x^n) = \prod_{j=1}^{a_i} F_{ij}(x)$ with $deg(F_{ij}) = D_i$ denote the prime factorization of $f_i(x^n)$ for $i = 1,2,\cdots,r$. Then

$$N(n,m,B) \begin{cases} \leq n^r & \text{if } k_i = 1 \text{ for } i = 1,2,\cdots,r \\ = n^m & \text{if } d_i = b_i = k_i = 1 \text{ and } a_i = n \text{ for } i = 1,2,\cdots,r \\ \text{either, 0 or } \geq \prod_{i=1}^{r} (q^{d_i}-1)^{k_i} & \text{if } b_i = 1, k_i \geq 2 \text{ and } D_i \mid k_i d_i \end{cases}$$

for $i = 1,2,\cdots,r$.

PROOF. Apply Lemmas 5 and 7 and Corollary 6.

REFERENCES

1. ACOSTA-DE-OROZCO, M.T. & GOMEZ-CALDERON, J., Matrix powers over finite fields, *Internat. J. Math. and Math. Sci.* **15** (4) (1992), 767-772.
2. DICKSON, L.E., *Linear Algebra*, Leipzig, 1901.
3. HODGES, J.H., Scalar polynomial equations for matrices over a finite field, *Duke Math. J.* **25** (1958), 291-296.
4. LANG, S., *Algebra*, Addison-Wesley, Reading, MA, 1971.
5. McDONALD, B.R., Involutory Matrices over finite local rings, *Canadian J. of Math.* **24** (1972), 369-378.

Mathematical Problems in Engineering

Special Issue on Time-Dependent Billiards

Call for Papers

This subject has been extensively studied in the past years for one-, two-, and three-dimensional space. Additionally, such dynamical systems can exhibit a very important and still unexplained phenomenon, called as the Fermi acceleration phenomenon. Basically, the phenomenon of Fermi acceleration (FA) is a process in which a classical particle can acquire unbounded energy from collisions with a heavy moving wall. This phenomenon was originally proposed by Enrico Fermi in 1949 as a possible explanation of the origin of the large energies of the cosmic particles. His original model was then modified and considered under different approaches and using many versions. Moreover, applications of FA have been of a large broad interest in many different fields of science including plasma physics, astrophysics, atomic physics, optics, and time-dependent billiard problems and they are useful for controlling chaos in Engineering and dynamical systems exhibiting chaos (both conservative and dissipative chaos).

We intend to publish in this special issue papers reporting research on time-dependent billiards. The topic includes both conservative and dissipative dynamics. Papers discussing dynamical properties, statistical and mathematical results, stability investigation of the phase space structure, the phenomenon of Fermi acceleration, conditions for having suppression of Fermi acceleration, and computational and numerical methods for exploring these structures and applications are welcome.

To be acceptable for publication in the special issue of Mathematical Problems in Engineering, papers must make significant, original, and correct contributions to one or more of the topics above mentioned. Mathematical papers regarding the topics above are also welcome.

Authors should follow the Mathematical Problems in Engineering manuscript format described at http://www.hindawi.com/journals/mpe/. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/ according to the following timetable:

Manuscript Due	March 1, 2009
First Round of Reviews	June 1, 2009
Publication Date	September 1, 2009

Guest Editors

Edson Denis Leonel, Department of Statistics, Applied Mathematics and Computing, Institute of Geosciences and Exact Sciences, State University of São Paulo at Rio Claro, Avenida 24A, 1515 Bela Vista, 13506-700 Rio Claro, SP, Brazil; edleonel@rc.unesp.br

Alexander Loskutov, Physics Faculty, Moscow State University, Vorob'evy Gory, Moscow 119992, Russia; loskutov@chaos.phys.msu.ru