Štefan Schwarz

Fermat's theorem for matrices revisited

Mathematica Slovaca, Vol. 35 (1985), No. 4, 343--347

Persistent URL: http://dml.cz/dmlcz/136402

Math. Slovaca 35, 1985, No. 4, 343—347

FERMAT'S THEOREM FOR MATRICES REVISITED

ŠTEFAN SCHWARZ

In all of the paper GF(q) denotes a finite field with $q=p^s$ elements ($s\geqq 1$, p a prime) and S_n is the multiplicative semigroup of all $n\times n$ matrices over GF(q).

Let $A\in S_n$ and consider the sequence $A, A^2, A^3, \ldots$ Denote by $A^{k(A)}$ the least power of A which appears in this sequence more than once. Denote by $k(A)+d(A)$ the least exponent for which $A^{k(A)}=A^{k(A)+d(A)}$ holds. It is well known that $A^{k(A)}, A^{k(A)+1}, \ldots, A^{k(A)+d(A)-1}$ is a cyclic group.

By Fermat's theorem for matrices we mean an identity of the form $A^{\varkappa}=A^{\varkappa+\delta}$ which holds for all $A\in S_n$ and the integers $\varkappa$ and δ are as small as possible.

We have almost immediately

$$\varkappa=\max\{k(A)|A\in S_n\},\quad \delta=\mathrm{LCM}\{d(A)|A\in S_n\}.$$

The first step in finding δ has been made by I. B. Marshall [3] in 1941. His result has been strenghtened by I. Niven [4] in 1948.

Denote for any integer $l\geqq 1$

$$\lambda(l, q)=p^t\cdot\mathrm{LCM}[q^l-1, q^{l-1}-1, \ldots, q-1],$$

where t is the least integer for which $p^t\geqq l$.

Denote further by D_n the group of all non-singular $n\times n$ matrices contained in S_n.

Marshall proved that for any $A\in D_n$ we have $A^{\lambda(n,q)}=E_n$, where E_n is the $n\times n$ unit matrix. Niven proved that the integer $\lambda(n, q)$ cannot be replaced by a smaller one. The number $\lambda(n, q)$ is the least common multiple of the orders of the elements of D_n. Note that there is no element in D_n of order $\lambda(n, q)$.

We summarize:

Lemma 1. (Marshall and Niven) *For any non-singular $n\times n$ matrix A over* GF(q) *we have $A=A^{1+\lambda(n,q)}$, and this is the best possible result.*

Explicitly: This is the best possible result in the sense that the integer $\lambda(n, q)$ cannot be replaced by a smaller one if we insist on the natural requirement to make the exponent independent of the special choice of A.

Recently in 1980 A. Klein [2] proved that for any $A\in S_n$ we have $A^n=A^{n+\lambda(n,q)}$ and neither n nor $\lambda(n, q)$ can be replaced by a smaller number.

The aim of this note is to give a new transparent proof of the result of Klein and to extend this result to singular matrices. In particular we show that for any matrix A with $1 \leqq \text{rank } (A) \leqq h \leqq n-1$ we have $A^{h+1} = A^{h+1+\lambda(h,q)}$ and this is the best possible result.

Our proof is a typical semigroup-theoretical proof. Hereby we use only rather elementary facts from the theory of semigroups, in particular two statements concerning completely 0-simple semigroups.

We shall use the following notation. If $A \in S_n$, and A is contained in a subgroup of S_n, then $G(A)$ denotes the maximal subgroup of S_n containing the matrix A.

Denote by I_h the two-sided ideal of the semigroup S_n consisting of all matrices A such that rank $(A) \leqq h$. We have the following chain

$$S_n = I_n \supset I_{n-1} \supset I_{n-2} \supset \ldots \supset I_1 \supset I_0 = 0,$$

and S_n has no other two-sided ideals.

Denote further $D_h = I_h - I_{h-1}$ $(h = 1, 2, \ldots, n)$. Then D_h is the set of all matrices of rank h.

Recall

$$\text{rank}(A) \geqq \text{rank}(A^2) \geqq \text{rank}(A^3) \geqq \ldots,$$

and if $\text{rank}(A^l) = \text{rank}(A^{l+1})$, then $\text{rank}(A^l) = \text{rank}(A^{l+u})$ for any $u \geqq 1$. Hence to any $A \in S_n$ there is an exponent l, $1 \leqq l \leqq n$, such that $\text{rank}(A^l) = \text{rank}(A^{l+1})$.

Let there be $1 \leqq h \leqq n-1$ and consider the set $\bar{D}_h = D_h \cup \{\bar{0}\}$, with the multiplication $\odot$ defined as follows. For $X, Y \in D_h$

$$X \odot Y = \begin{cases} XY & \text{if} \quad XY \in D_h, \\ \bar{0} & \text{if} \quad XY \notin D_h, \end{cases}$$

and $\bar{0}$ has the usual properties of a multiplicative zero. (In the usual terminology $\bar{D}_h$ is the factor semigroup I_h/I_{h-1}.) $\bar{D}_h$ is a finite 0-simple semigroup. It is well known from the elements of the theory of semigroups that for any $A \in \bar{D}_h$, $A \neq \bar{0}$, either A is contained in a group [hence in $G(A)$] or $A^2 = \bar{0}$. (See [1].) The first case takes place if and only if $\text{rank}(A) = \text{rank}(A^2)$. Moreover (as in any finite 0-simple semigroup) all maximal groups contained in D_h are isomorphic.

a) Suppose first that $A \in D_h$ and $\text{rank}(A) = \text{rank}(A^2)$, hence $A \in G(A)$. We need some informations concerning the group $G(A)$. Since all maximal groups contained in D_h are isomorphic we may consider the maximal group $G(E_h)$, where

$$E_h = \text{diag}(\underbrace{1, 1, \ldots, 1}_{h\text{-times}}, 0 \ldots 0).$$

If $B \in G(E_h)$, then $B = E_h B E_h$. Write $B = \begin{pmatrix} B_1 & C \\ D & F \end{pmatrix}$, where B_1 is an $h \times h$ matrix.

The equality

$$E_h\begin{pmatrix} B_1 & C \\ D & F \end{pmatrix} E_h = \begin{pmatrix} B_1 & C \\ D & F \end{pmatrix}$$

holds if and only if C, D, F are rectangular zero matrices. Hereby B_1 is a non-singular $h \times h$ matrix (since otherwise B would not be contained in D_h). Hence any $B \in G(E_h)$ is of the form $\begin{pmatrix} B_1 & 0 \\ 0 & 0 \end{pmatrix}$ with a non-singular $h \times h$ matrix B_1. Conversely, the set of all $n \times n$ matrices of this form is a group. Hence $G(E_h)$ consists of all matrices of this form. By Lemma 1 we have $B^{\lambda(h,q)} = E_h$ and $\lambda(h, q)$ cannot be replaced by a smaller integer. This implies $B = B^{1+\lambda(h,q)}$ for any $B \in G(E_h)$. With respect to the isomorphism of $G(A)$ and $G(E_h)$ we have $A = A^{1+\lambda(h,q)}$ for any $A \in G(A) \subset D_h$, and this is the best possible result.

b) Suppose next $A \in D_h$ and $\operatorname{rank}(A) > \operatorname{rank}(A^2)$, hence $h < n$. Let l_0, $2 \leqq l_0 \leqq h+1$, be the least integer such that $\operatorname{rank}(A^{l_0}) = \operatorname{rank}(A^{l_0+1})$. Denote $h_1 = \operatorname{rank}(A^{l_0}) < h$. Then $A^{l_0} \in G(A^{l_0})$ and this maximal group is contained in D_{h_1}. If u is the order of the group element A^{l_0} in $G(A^{l_0})$, we have $A^{l_0} = A^{l_0+u}$. Now any group element in D_{h_1} has an order which is a divisor of $\lambda(h_1, q)$. Hence

$$A^{l_0} = A^{l_0+\lambda(h_1,q)}.$$

Multiplying by A^{h+1-l_0} we obtain

$$A^{h+1} = A^{h+1+\lambda(h_1,q)}. \tag{1}$$

Here $h_1 < h$. [Note explicitly that (1) holds only in the case b).]

Since $h_1 < h$, we have $\lambda(h_1, q)/\lambda(h, q)$, and (1) implies

$$A^{h+1} = A^{h+1+\lambda(h,q)}. \tag{2}$$

The result (2) holds also in the case a), since $A = A^{1+\lambda(h,q)}$ implies (2). Hence (2) holds for all $A \in D_h$.

We now show that (2) is the best possible result which holds for all $A \in D_h$.

The exponent $\lambda(h, q)$ cannot be replaced by a smaller one. For, if $A \in G(A)$ and $A^{h+1} = A^{h+1+u}$, then $A = A^{1+u}$, hence [by a)] $u \geqq \lambda(h, q)$.

We next show that there is a B such $B^h \neq B^{h+\lambda(h,q)}$. Consider the $n \times n$ matrix $B = \begin{pmatrix} U & 0 \\ 0 & 0 \end{pmatrix}$, where U is the $(h+1) \times (h+1)$ matrix

$$U = \begin{pmatrix} 0 & 1 & 0 \dots 0 \\ 0 & 0 & 1 \dots 0 \\ \vdots & & \\ 0 & 0 & 0 \dots 1 \\ 0 & 0 & 0 \dots 0 \end{pmatrix}.$$

Here $\operatorname{rank}(B)=h$, next $B^h \neq 0$, while $B^{h+1}=B^{h+2}=\ldots=B^{h+\lambda(h,q)}=0$. Hence in (2) the exponent $h+1$ cannot be replaced by h.

We have proved:

Theorem. *For any $n \times n$ matrix A over* $\mathrm{GF}(q)$, *with* $1 \leqq \operatorname{rank}(A) \leqq h \leqq n-1$, *we have*

$$A^{h+1}=A^{h+1+\lambda(h,q)},$$

and this result is the best possible.

Explicitly: The best possible in the sense that neither $h+1$ nor $\lambda(h, q)$ can be replaced by a smaller number if we insist on the requirement that the exponents should be independent of the special choice of $A \in I_h$.

In other words: The polynomial $x^{u+v}-x^u$ with smallest u and v "vanishing" for all $A \in I_h$ is the polynomial $x^{h+1+\lambda(h,q)}-x^{h+1}$.

For any individual matrix $A \in I_h$ there is always a number $u(A)$ such that $u(A)/\lambda(h, q)$, $u(A)<\lambda(h, q)$, and $A^{h+1}=A^{h+1+u(A)}$.

In the case of $h=n-1$ we obtain:

Corollary 1. *For any $n \times n$ singular matrix over* $\mathrm{GF}(q)$ *we have*

$$A^n=A^{n+\lambda(n-1,q)}, \tag{3}$$

and this result is the best possible.

If $A \in D_n$, then $A^{\lambda(n,q)}=E_n$ implies $A^n=A^{n+\lambda(n,q)}$ and this together with (3) implies the result of Klein [2].

Corollary 2. *For any $n \times n$ matrix $A \in S_n$ we have*

$$A^n=A^{n+\lambda(n,q)} \tag{4}$$

and this is the best possible result.

Corollary 3. *For any $n \times n$ matrix over* $\mathrm{GF}(q)$ *with* $1 \leqq \operatorname{rank}(A) \leqq h$, *the matrix* $A^{\lambda(h,q)}$ *is an indempotent matrix.*

Proof. If $\operatorname{rank}(A)=n$, this idempotent is E_n. Suppose $1 \leqq h \leqq n-1$. Then

$$\lambda(h, q)=p^t \operatorname{LCM}[q^h-1, q^{h-1}-1, \ldots, q-1] \geqq n \cdot 1 \geqq h+1.$$

Multiplying (2) by $A^{\lambda(h,q)-(h+1)}$ we obtain $A^{\lambda(h,q)}=A^{2\lambda(h,q)}$, which proves our statement.

Here again $\lambda(h, q)$ is the least integer r such that $X^r=X^{2r}$ holds for all $X \in I_h$.

A numerical example. Consider the ring (or semigroup) of all 4×4 matrices over GF(3). We have:

$$\lambda(4, 3)=3^2 \cdot \operatorname{LCM}[3^4-1, 3^3-1, 3^2-1, 3-1]=9360,$$
$$\lambda(3, 3)=3 \cdot \operatorname{LCM}[3^3-1, 3^2-1, 3-1]=312,$$

$$\lambda(2, 3)=3\cdot\text{LCM}\,[3^2-1, 3-1]=24,$$
$$\lambda(1, 3)=3^0\cdot(3-1)=2.$$

This implies:

$$A^4=A^{9364} \quad \text{if} \quad \text{rank}(A)\leqq 4,$$
$$A^4=A^{316} \quad \text{if} \quad \text{rank}(A)\leqq 3,$$
$$A^3=A^{27} \quad \text{if} \quad \text{rank}(A)\leqq 2,$$
$$A^2=A^4 \quad \text{if} \quad \text{rank}(A)\leqq 1.$$

Remark. The result of this paper was announced (among other results) in a short communication given at the ICM 1978 at Helsinki.

REFERENCES

[1] CLIFFORD, A. H.—PRESTON, G. B.: The Algebraic Theory of Semigroups I. Amer. Math. Soc., Providence R. I., 1961.

[2] KLEIN, A.: On Fermat's theorem for matrices and the periodic identities of M_n [GF(q)]. Archiv d. Math. 34, 1980, 399—402.

[3] MARSHALL, I. B.: On the extension of Fermat's theorem to matrices of order n. Proceedings of the Edinburgh Math. Soc. 6, 1939—1941, 85—91.

[4] NIVEN, I.: Fermat's theorem for matrices. Duke Math. J. 15, 1948, 823—826.

Received May 25, 1983

Matematický ústav SAV
Obrancov mieru 49
814 73 Bratislava

ТЕОРЕМА ФЕРМА ДЛЯ МАТРИЦ, ЕЩЁ ОДИН РАЗ

Štefan Schwarz

Резюме

Пусть $A - n\times n$ матрица над конечным полем GF(q). Доказывается: Для всякого A, для которого $1\leqq\text{rank}(A)\leqq h$ и $h<n$, имеет место равенство (2). В этом равенстве нельзя ни h ни $\lambda(h, q)$ заменять меньшим числом. Функция $\lambda(h, q)$ введена в тексте. Если $h=n$, то имеет место (4).