Czechoslovak Mathematical Journal

Štefan Schwarz

The Euler-Fermat theorem for the semigroup of circulant Boolean matrices

Czechoslovak Mathematical Journal, Vol. 30 (1980), No. 1, 135–141

Persistent URL: http://dml.cz/dmlcz/101663

Czechoslovak Mathematical Journal, 30 (105) 1980, Praha

THE EULER-FERMAT THEOREM FOR THE SEMIGROUP OF CIRCULANT BOOLEAN MATRICES

ŠTEFAN SCHWARZ, Bratislava

(Received June 29, 1978)

Let S be a finite semigroup and $a \in S$. The sequence

$$a, a^2, a^3, \dots \tag{1}$$

has only a finite number of different elements. Denote by $k = k(a)$ the smallest natural number k for which $a^k = a^l$ for some $l > k$. Denote further by $k + d$, $d = d(a) \geqq 1$ the least exponent for which $a^k = a^{k+d}$ holds. Then the sequence (1) is of the form

$$a, a^2, \dots, a^{k-1} | a^k, \dots, a^{k+d-1} | \, a^k, \dots . \tag{2}$$

It is well known that $\{a^k, \dots, a^{k+d-1}\}$ is a cyclic group of order d.

To any $a \in S$ we have associated two integers $k(a), d(a)$ and we have $a^{k(a)} = a^{k(a)+d(a)}$.

Denote $K = \max \{k(a) \mid a \in S\}$ and $D = \text{l.c.m.} \{d(a) \mid a \in S\}$. Then $K = K(S)$ and $D = D(S)$ are characteristics of the semigroup S and for any $a \in S$ we have

$$a^K = a^{K+D} . \tag{3}$$

Hereby K and D are the least integers having this property (if we insist on the natural requirement that K and D should be independent of a).

The identity (3) may be called the Euler-Fermat Theorem for the semigroup S.

To explain this name suppose that p is a prime and S_p is the multiplicative semigroup of residue classes (mod p). Then for any $a \in S_p$ we have $a = a^p$. Here $K = 1$ and $D = p - 1$.

There is a rather limited number of important semigroups (playing a role in various parts of mathematics) for which the exact values of $K = K(S)$ and $D = D(S)$ are known. We mention two of them.

1. Let $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ be the factorization of the integer $n > 1$ into the product of primes and S_n the multiplicative semigroup of residue classes (mod n).

Denote $\nu(n) = \max(\alpha_1, \alpha_2, \ldots, \alpha_r)$. Let $\lambda(n)$ be the Carmichael function, i.e.

$$\lambda(n) = \text{l.c.m.}\ [\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})]\,,$$

where

$$\lambda(p^\alpha) = \begin{cases} 2^{\alpha-2} & \text{for} \quad p = 2 \quad \text{and} \quad \alpha > 2\,, \\ p^{\alpha-1}(p-1) & \text{otherwise}\,. \end{cases}$$

We then have: $K(S_n) = \nu(n)$ and $D(S_n) = \lambda(n)$. Hence we have: $a^{\nu(n)} = a^{\nu(n)+\lambda(n)}$ for any $a \in S_n$ and none of the exponents can be replaced by a smaller number. (This is the best possible generalization of Euler's Theorem from the elementary theory of numbers.)

2. By an $n \times n$ Boolean matrix $(n > 1)$ we mean an $n \times n$ matrix over the semiring $\{0, 1\}$ under the operations $a + b = \sup(a, b)$, $a \,.\, b = \min(a, b)$.

Denote by B_n the multiplicative semigroup of all Boolean matrices. Clearly $\text{card}\, B_n = |B_n| = 2^{n^2}$ and B_n is isomorphic to the multiplicative semigroup of all binary relations on a finite set X with $|X| = n$.

In this case it is known that $K(B_n) = (n-1)^2 + 1$. $D(B_n)$ is a function of n which can be computed in the following way. Let $n = n_1 + n_2 + \ldots + n_s$ be a partition of n. Then $D(B_n) = \max\{\text{l.c.m.}\ [n_1, n_2, \ldots, n_s]\}$, where $(n_1, n_2, \ldots, n_s)$ runs through all possible partitions of n. Otherwise expressed:

$D(B_n)$ is the largest order of an element in the group of all permutations of n elements.

E.g., if $n = 5$, we have $K(B_5) = 17$, $D(B_5) = 6$ and for any $A \in B_5$ we have $A^{17} = A^{23}$. Hereby none of the exponents can be replaced by a smaller number.

1

In this paper we shall deal with the multiplicative semigroup of all circulant Boolean matrices of order n.

A circulant is a Boolean matrix of the form

$$\begin{pmatrix} a_0, & a_1, & \ldots, & a_{n-1} \\ a_{n-1}, & a_0, & \ldots, & a_{n-2} \\ \ldots & \ldots & \ldots & \ldots \\ a_1, & a_2, & \ldots, & a_0 \end{pmatrix},$$

where $a_i \in \{0, 1\}$. Denote by

$$P = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

and let E be the unit matrix of order n. Then any circulant can be written in the form

$$A = a_0E + a_1P + a_2P^2 + \ldots + a_{n-1}P^{n-1}\,, \quad a_i \in \{0, 1\}\,. \tag{4}$$

We have $P^n = E$ and for convenience we also define $P^0 = E$.

The set of all circulants of order n is (under multiplication) a semigroup C_n with $|C_n| = 2^n$ (including the zero circulant Z). Note that C_n contains the cyclic group $G_n = \{E, P, \ldots, P^{n-1}\}$.

If $A = (a_{ij})$ and $B = (b_{ij})$ are Boolean matrices, we denote by $A \cap B$ the matrix $D = (d_{ij})$ with $d_{ij} = \min(a_{ij}, b_{ij})$. We shall write $A \leqq B$ if and only if $A \cap B = A$. Clearly, if $j \neq l \pmod{n}$, we have $P^j \cap P^l = Z$, which implies that any element $\in C_n$ has a unique representation in the form (4).

The following is the Euler-Fermat Theorem for the semigroup C_n.

Theorem 1. *For any $A \in C_n$ we have*

$$A^{n-1} = A^{2n-1}\,. \tag{5}$$

This result is the best possible, i.e. none of the exponents can be replaced by a smaller number.

Proof. a) If $A = Z$, (5) is trivially true. If $A = P^j$ $(0 \leqq j \leqq n-1)$, (5) is true, since

$$P^{j(2n-1)} = P^{j(n-1)}P^{jn} = P^{j(n-1)}\,. \tag{6}$$

b) Suppose next that A is of the form

$$A = E + P^{j_1} + P^{j_2} + \ldots + P^{j_k}\,, \quad 1 \leqq j_1 < j_2 < \ldots < j_k \leqq n-1\,.$$

In this case we have $A = EA \leqq A\,.\,A = A^2$. Now $A \leqq A^2$ implies $A \leqq A^2 \leqq \leqq A^3 \leqq \ldots \leqq A^{n-1} \leqq A^n$. Since $j_1 \geqq 1$, the first row of A (hence any row of A) contains at least two non-zero elements. The matrix A^2 is either A or it contains at least three non-zero elements in each of the rows. Repeating this argument we obtain: There is an integer $h \leqq n-1$ such that $A^h = A^{h+1}$. The more $A^{n-1} = A^n = = A^{n+1} = \ldots = A^{2n-1}$, which implies $A^{n-1} = A^{2n-1}$.

c) Suppose finally that A is of the form $A = P^jB$, where

$$B = E + P^{j_1} + \ldots + P^{j_k}\,, \quad 1 \leqq j_1 < j_2 < \ldots \leqq n-1\,.$$

Then with respect to (6)

$$A^{2n-1} = (P^jB)^{2n-1} = P^{j(2n-1)}B^{2n-1} = P^{j(n-1)}B^{n-1} = (P^jB)^{n-1} = A^{n-1}\,.$$

This proves (5) in all cases.

d) Consider the element $B = E + P \in C_n$. Then for any $u \geqq n - 1$ we have $B^u = B^{n-1} = E + P + \ldots + P^{n-2} + P^{n-1} = J$, where J is the $n \times n$ matrix with all elements equal to 1. On the other hand $B^{n-2} = E + P + \ldots + P^{n-2} \neq J$. Hence $B^{n-2} \neq B^u$ for any $u \geqq n - 1$.

e) Consider next the element $B = P$. We have $P^{n-1} = P^{2n-1}$, but for all v satisfying $n - 1 < v < 2n - 1$ we have $P^{n-1} \neq P^v$. This completes the proof of Theorem 1.

2

The identity (5) holds for all $A \in C_n$. Modified results can be obtained if we specify "the position" of A in C_n.

To prove the corresponding results we need some informations concerning the structure of the semigroup C_n.

In [1] we have proved: If d is a divisor of n, $n = dt$, then

$$E^{(d)} = E + P^d + P^{2d} + \ldots + P^{(t-1)d}$$

is an idempotent $\in C_n$ and any idempotent $\in C_n$ different from Z can be obtained in this manner. (Note that in this notation $E^{(n)} = E$ and $E^{(1)} = J$.)

Denote by K_d the set of all $A \in C_n$ such that $A^s = E^{(d)}$ for some integer $s \geqq 0$ (depending on A). Then $C_n - Z = \bigcup_{d|n} K_d$ is a union of disjoint subsemigroups of C_n. We call K_d the maximal subsemigroup of C_n belonging to the idempotent $E^{(d)}$. (It is largest subsemigroup of C_n containing $E^{(d)}$ and no other idempotents.)

The maximal group containing $E^{(d)}$ as its unit element is the group $G_d = \{E^{(d)}, P \,.\, E^{(d)}, \ldots, P^{d-1}E^{(d)}\}$, a cyclic group of order d. Clearly $G_d \subset K_d$. In particular $K_n = G_n = \{E, P, P^2, \ldots, P^{n-1}\}$, while G_1 is the one point group $G_1 = \{J\}$.

Note also that the set of all idempotents $\in C_n$ different from Z becomes a modular lattice if we define

$$E^{(d_1)} \vee E^{(d_2)} = E^{([d_1,d_2])} \quad \text{and} \quad E^{(d_1)} \wedge E^{(d_2)} = E^{((d_1,d_2))},$$

where $[d_1, d_2]$ and (d_1, d_2) denote the least common multiple and the greatest common divisor of d_1 and d_2 respectively.

Example. Let $n = 45$. The semigroup C_{45} contains 6 idempotents different from Z. In the schematic figure 1 each square denotes a maximal subsemigroup of C_{45}. The circle contained in K_d is the maximal group G_d with unit element $E^{(d)}$.
We have $C_{45} - Z = K_{45} \cup K_{15} \cup K_9 \cup K_5 \cup K_3 \cup K_1$. Consider, e.g., $d = 15$. We have $E^{(15)} = E + P^{15} + P^{30}$ and $G_{15} = \{E^{(15)}, PE^{(15)}, \ldots, P^{14}E^{(15)}\}$. K_{15} is the set of all $Y \in C_{45}$ for which $Y^s = E + P^{15} + P^{30}$ for some integer $s \geqq 1$. In [2] (p. 509) an explicit formula for the number $|K_d|$ has been given, namely $|K_d| = d \sum_{j|t} j\, \mu(j)\, (2^{t/j} - 1)$, where $t = n/d$ and $\mu(j)$ is the Möbius function. From this formula we obtain $|K_{15}| = 60$.

Note also that $|K_1| = (2^{45} - 1) - 3(2^{15} - 1) - 5(2^9 - 1) + 15(2^3 - 1)$, so that by far the most elements $\in C_{45}$ are contained in K_1. It can be easily shown that

$$\lim_{n=\infty} \frac{|K_1|}{2^n} = 1 .$$

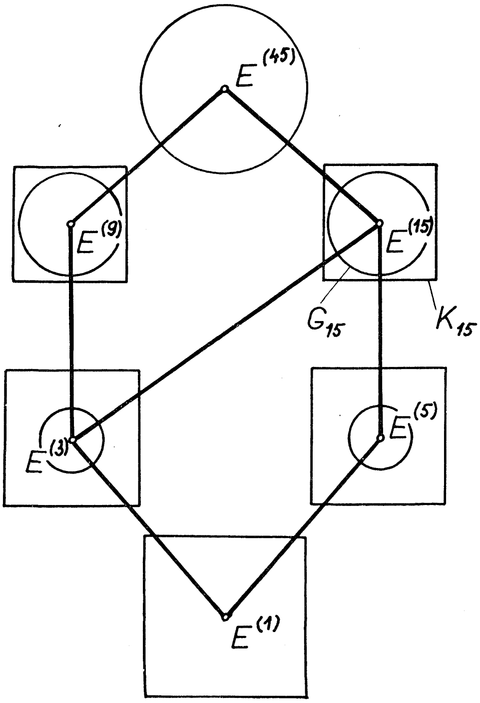

Fig. 1.

3

The aim of this section is the proof of Theorem 3, which is the Euler-Fermat Theorem for the semigroup K_d. It turns out that if we specify that $A \in K_d$, then the exponents in (5) can be replaced by smaller numbers.

Theorem 2 may be considered as a supplement to the results obtained in [1] and [2].

Theorem 2. *For any $A \in K_d$, $d \neq n$, we have $A^{n/d-1} \in G_d$ and the number $n/d - 1$ cannot be replaced by a smaller one.*

Remark. If $d = n$, we have $K_d = G_d$ and the statement formally holds if we define $A^0 = E$.

Proof. Write $t = n/d$. In [2] we have proved that any element $\in K_d$ can be written in the form

$$A = P^l(E + P^{u_1 d} + P^{u_2 d} + \ldots + P^{u_k d}),$$

where $1 \leqq u_1 < u_2 < \ldots < u_k \leqq t - 1$ and $0 \leqq l \leqq n - 1$. Note that not all possible choices of $u_1, u_2, \ldots, u_k$ are giving elements $\in K_d$ (some of them are elements $\in K_j$ where d is a divisor of j).

a) Denote $B = E + P^{u_1 d} + \ldots + P^{u_k d}$ and note that if $B \in K_d$, we also have $P^l B \in K_d$. We have again $B \leqq B^2$ which implies $B \leqq B^2 \leqq B^3 \leqq \ldots \leqq B^h$. By assumption B belongs to the idempotent $E^{(d)}$ and $E^{(d)}$ contains in each row exactly t non-zero elements. Analogously as in the proof of Theorem 1 we conclude that there is an integer $h \leqq t - 1$ such that $B^h = B^{h+1}$. Hence B^h is an idempotent $\in C_n$ and therefore $B^h = E^{(d)} \in G_d$.

b) Suppose next $1 \leqq l \leqq n - 1$ and $A = P^l B$. Then with the same h as sub a) we have $A^h = P^{lh} = P^{lh} E^{(d)}$, which is an element $\in G_d$.

c) To see that $t - 1$ cannot be replaced by a smaller number consider the element $Y = E + P^d \in C_n$. We have $Y \in K_d$,

$$Y^{t-2} = (E + P^d)^{t-2} = E + P^d + \ldots + P^{d(t-2)} \neq E^{(d)}.$$

If Y^{t-2} were an element $\in G_d$, we would have $Y^{t-2}E^{(d)} = Y^{t-2}$. Now $Y^{t-2}E^{(d)} = (E + P + \ldots + P^{d(t-2)})(E + P^d + \ldots + P^{d(t-1)}) = E^{(d)}$. Since $Y^{t-2} \neq E^{(d)}$, we have a contradiction. Hence Y^{t-2} is not an element $\in G_d$. This proves Theorem 2.

Theorem 3. *For any $A \in K_d$, $d \neq n$, we have*

$$A^{n/d-1} = A^{n/d-1+d}.$$

None of the exponents can be replaced by a smaller integer.

Remark. For $A \in K_n = G_n$ we have $E = A^n$. The statement of the Theorem is true if we define $A^0 = E$.

Proof. a) Put again $t = n/d$. Let $A \in K_d$ and consider the sequence $A, A^2, A^3, \ldots$. Since A^{t-1} is in the group G_d, recalling (2), we immediately see that $A^t, A^{t+1}, \ldots$ are contained in the group G_d. Since G_d is of order d we have $A^{t-1} = A^{t-1+d}$.

b) The exponent on the left hand side cannot be replaced by $t - 2$ since $(E + P^d)^{t-2}$ is not contained in G_d while all powers $(E + P^d)^l$ with $l \geqq t - 1$ are elements of the group G_d. (As a matter of fact for $l \geqq t - 1$ $(E + P^d)^l = E^{(d)}$.)

c) The exponent on the right hand side cannot be replaced by a smaller one, i.e. $A^{t-1} = A^{t-1+u}$, $1 \leqq u < d$, does not hold for all $A \in K_d$. It is sufficient to put $A = PE^{(d)}$. We have $A^{t-1+u} = P^{t-1+u}E^{(d)} \neq P^{t-1}E^{(d)} = A^{t-1}$. This proves Theorem 3.

Example (continued). For the semigroup C_{45} we obtain by Theorem 3 the following identities:

$$\begin{aligned}
E &= A^{45} \quad \text{for} \quad A \in K_{45}, & A^8 &= A^{13} \quad \text{for} \quad A \in K_5, \\
A^2 &= A^{17} \quad \text{for} \quad A \in K_{15}, & A^{14} &= A^{17} \quad \text{for} \quad A \in K_3, \\
A^4 &= A^{13} \quad \text{for} \quad A \in K_9, & A^{44} &= A^{45} \quad \text{for} \quad A \in K_1.
\end{aligned}$$

The best result holding for all $A \in C_{45}$ is (in accordance with Theorem 1) $A^{44} = A^{89}$.

References

[1] *K. K. Hang Butler* and *Š. Schwarz:* The semigroup of circulant Boolean matrices, Czechoslovak Math. J. *26* (101) (1976), 632–635.

[2] *Š. Schwarz:* A counting theorem in the semigroup of circulant Boolean matrices, Czechoslovak Math. J. *27* (102) (1977), 504–510.

Author's address: 880 19 Bratislava, Gottwaldovo nám. 19, ČSSR (Slovenská vysoká škola technická).