Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2024, Volume 30, Number 1, 116–140
DOI: 10.7546/nntdm.2024.30.1.116-140

Sequences in finite fields yielding divisors of Mersenne, Fermat and Lehmer numbers, I

A. M. S. Ramasamy

Department of Mathematics, Pondicherry University
Pondicherry – 605014, India
e-mail: amsramasamy@gmail.com

Received: 25 August 2023 **Revised:** 4 March 2024
Accepted: 6 March 2024 **Online First:** 7 March 2024

Abstract: The aim of this work is to present a method using the cyclic sequences $\{M_k\}, \{\theta_{t,k}\}$ and $\{\psi_{t,k}\}$ in the finite fields $\mathbb{F}_\rho$, with ρ a prime, that yield divisors of Mersenne, Fermat and Lehmer numbers. The transformations τ_t and σ_t are introduced which lead to the proof of the cyclic nature of the sequences $\{\theta_{t,k}\}$ and $\{\psi_{t,k}\}$. Results on the roots of the $H(x)$-polynomials in $\mathbb{F}_\rho$ form the central theme of the study.
Keywords: Satellite polynomials, $M-$cycle, Background prime, The transformations τ_t and σ_t, Symmetric and skew-symmetric properties, Pivotal elements, Euler's totient function.
2020 Mathematics Subject Classification: 11A51, 11B50, 11C08, 11T06.

1 Introduction

Fermat (1601–1665) considered a sequence of numbers of the form 2^m+1, where m is of the form 2^n. Since the few initial terms of this sequence yielded prime numbers successively, Fermat was under the impression that he had really obtained a formula for primes. It was Euler (1707–1783) who detected a flaw in the concept of Fermat when he found the divisibility of the number $2^{32}+1$ by 641. Numbers of the form $2^{2^n}+1$ $(n \geq 0)$ are called the Fermat numbers.

Numbers of the form 2^n-1 are referred to as Mersenne numbers and primes of this form are called Mersenne primes, named after Fr.Martin Mersenne (1588–1648). A necessary condition

for the number $2^n - 1$ to be a prime is that n shall be a prime (see, for e.g., Hardy and Wright [3]). Brillhart [1], Brillhart and Johnson [2], Kang [4], and Kravitz [5] have presented certain results on the divisors of Mersenne numbers. There is another type of numbers of interest. Numbers of the form $2^n + 1$ are named after Lehmer, as per a reference by Ribenboim in [9]. It turns out that Fermat numbers are particular cases of Lehmer numbers. Leyendekkers and Shannon [6] have brought out certain remarkable properties of Mersenne and Fermat numbers.

In the sequel, it is established that certain cyclic sequences in the finite fields $\mathbb{F}_\rho$, with ρ a prime, yield the divisors of Mersenne, Fermat and Lehmer numbers. The main results of this study are contained in Theorems 2.12, 2.14, 3.1, 3.4, 4.6, 5.5, Corollary 5.4, Theorems 6.1, 7.10, 8.2 and 8.3.

2 The sequences of polynomials over $\mathbb{Z}$

Notations. Let N and $\mathbb{Z}$ denote the sets of natural numbers and integers, respectively.

Problem of motivation. To settle the question concerning the common solutions of two Pell's equations, the concept of the characteristic number of two simultaneous Pell's equations was introduced by Mohanty and the author in [7]. A generalized version of this method was presented by the author in [8]. Two functions viz. $a(t)$ and $b(t)$ were introduced in [7] as follows: Let t be a natural number. Define $a(t) = A_{2^{t-1}}$ and $b(t) = B_{2^{t-1}}$, where $A_r + B_r\sqrt{D}$ denotes a solution of the Pell's equation $A^2 - DB^2 = 1$, D being a square-free natural number. The properties possessed by these functions was the focus of attention in [8]. These functions satisfy the relations $a(t+1) = 2(a(t))^2 - 1$ and $b(t+1) = 2a(t)b(t)$. The first relation implies $2a(t+1) = (2a(t))^2 - 2$. This property was the motivating point for the present work. As a consequence, certain polynomial sequences in $\mathbb{Z}[x]$ are introduced in this section.

Definition 2.1. (The polynomial sequence $\{F_k(x)\}$ in $\mathbb{Z}[x]$). *Define the infinite sequence* $\{F_k(x)\}$ *($k \geq 1$) in* $\mathbb{Z}[x]$ *as follows:*

$$F_1(x) = x \text{ and } F_{k+1}(x) = (F_k(x))^2 - 2, \forall\ k \in N. \tag{2.1}$$

Then we have

$$\begin{aligned} F_2(x) &= x^2 - 2, \\ F_3(x) &= x^4 - 4x^2 + 2, \\ F_4(x) &= x^8 - 8x^6 + 20x^4 - 16x^2 + 2, \\ F_5(x) &= x^{16} - 16x^{14} + 104x^{12} - 352x^{10} + 660x^8 - 672x^6 + 336x^4 - 64x^2 + 2, etc. \end{aligned}$$

By Eisenstein's criterion, it follows that the F_k(x)'s are irreducible over $\mathbb{Z}$ for $k \geq 2$.

Definition 2.2. (The polynomial sequences $\{G_k(x)\}$ and $\{H_k(x)\}$ in $\mathbb{Z}[x]$). *Define the infinite sequences* $\{G_k(x)\}$ *and* $\{H_k(x)\}$ *($k \geq 0$) over* $\mathbb{Z}$ *as follows:*

$$\left\{ \begin{array}{rcl} G_0(x) &=& 1,\ H_0(x) = 1, \\ G_{k+1}(x) &=& \frac{1}{2}\{xG_k(x) + (x-2)H_k(x)\}, \\ H_{k+1}(x) &=& \frac{1}{2}\{(x+2)G_k(x) + xH_k(x)\}\ (k \geq 0) \end{array} \right. . \tag{2.2}$$

Equivalently we have

$$G_0(x) = 1,\ G_1(x) = \ x - 1,\ G_{k+2}(x) = xG_{k+1}(x) - G_k(x)\ (k \geq 0), \tag{2.3}$$

$$H_0(x) = 1,\ H_1(x) = x + 1,\ H_{k+2}(x) = xH_{k+1}(x) - H_k(x)\ (k \geq 0). \tag{2.4}$$

Definition 2.3 (Matrix of polynomials)**.** *We define a matrix with two rows contributed by the sequences* $\{G_k(x)\}$ *and* $\{H_k(x)\}$ *as follows:*

$$\mathfrak{a}(x) = \begin{pmatrix} G_0(x) & G_1(x) & G_2(x) & \cdots \\ H_0(x) & H_1(x) & H_2(x) & \cdots \end{pmatrix}. \tag{2.5}$$

2.1 Properties of the polynomial sequences

Several properties of the sequences under consideration can be established by the method of induction. We obtain some identities.

Theorem 2.1. *The following relations hold:*

$$H_k(x) - G_k(x) = G_{k-1}(x) + H_{k-1}(x), \quad \textit{for all } k \geq 1. \tag{2.6}$$

$$G_{m+k}(x) + H_{m+k}(x) = G_m(x)H_k(x) + G_k(x)H_m(x), \quad \textit{for all } \ m, k \geq 0. \tag{2.7}$$

$$G_{2k}(x) + H_{2k}(x) = \ 2\, G_k(x)H_k(x), \quad \textit{for all } k \geq 0. \tag{2.8}$$

2.2 Determinants of sub-matrices of $\mathfrak{a}(x)$

We consider determinants of 2×2 sub-matrices of $\mathfrak{a}(x)$. By induction, the following property possessed by the elements in any two successive columns of $\mathfrak{a}(x)$ is got, using (2.3) and (2.4):

Theorem 2.2. *The following results hold:*

$$\begin{vmatrix} G_k(x) & G_{k+1}(x) \\ H_k(x) & H_{k+1}(x) \end{vmatrix} = 2,\ \forall\ k \geq 0, \tag{2.9}$$

$$\begin{vmatrix} G_k(x) & G_{k+r}(x) \\ H_k(x) & H_{k+r}(x) \end{vmatrix} = G_{r-1}(x) + H_{r-1}(x),\ \forall\ k \geq 0,\ r \geq 1. \tag{2.10}$$

2.3 Inter relationships among the terms of the sequences

Theorem 2.3. *For all integers* $k \geq 1$*, we have:*

$$\{G_{k-1}(x)\}^2 + \{G_k(x)\}^2 = xG_{k-1}(x)G_k(x) - x + 2, \tag{2.11}$$

$$\{H_{k-1}(x)\}^2 \ + \{H_k(x)\}^2 = xH_{k-1}(x)H_k(x) + x + 2, \tag{2.12}$$

$$x\{G_{k-1}(x)H_k(x) + \ G_k(x)H_{k-1}(x)\} = 2\{G_{k-1}(x)H_{k-1}(x) + \ G_k(x)H_k(x)\}, \tag{2.13}$$

$$G_{k+1}(x)H_{k+1}(x) = (x^2-1)G_k(x)H_k(x) - \frac{1}{2}xk\{G_{2k-1}(x) + \ H_{2k-1}(x)\}, \tag{2.14}$$

$$G_{2k+1}(x) + H_{2k+1}(x) = \ 2\ x\ G_k(x)H_k(x) - \{G_{2k-1}(x) + H_{2k-1}(x)\}\ . \tag{2.15}$$

Theorem 2.4. *The following relationships hold for all integers $k \geq 0$:*

$$\{G_{k+1}(x)\}^2 - G_k(x)G_{k+2}(x) = 2 - x, \tag{2.16}$$

$$\{H_{k+1}(x)\}^2 - H_k(x)H_{k+2}(x) = 2 + x, \tag{2.17}$$

$$G_k(x)H_{k+2}(x) + G_{k+2}(x)H_k(x) = 2G_{k+1}(x)H_{k+1}(x), \tag{2.18}$$

$$\{G_{k+1}(x) + H_{k+1}(x)\}^2 - \{G_k(x) + H_k(x)\}\{G_{k+2}(x) + H_{k+2}(x)\} = 4. \tag{2.19}$$

2.4 Factorization results for polynomials

By repeated application of (2.3) and (2.4), we obtain

Theorem 2.5 (Reduction formulae)**.** *For $r < s$, we have*

$$G_s(x) = \frac{1}{2}\{G_r(x) + H_r(x)\}G_{s-r}(x) - \frac{1}{2}\{G_{r-1}(x) + H_{r-1}(x)\}G_{s-r-1}(x), \tag{2.20}$$

$$H_s(x) = \frac{1}{2}\{G_r(x) + H_r(x)\}H_{s-r}(x) - \frac{1}{2}\{G_{r-1}(x) + H_{r-1}(x)\}H_{s-r-1}(x). \tag{2.21}$$

Corollary 2.1. *The following results hold:*

$$G_{3j+1}(x) = \frac{1}{2}\{G_{2j}(x) + H_{2j}(x)\}G_{j+1}(x) - \frac{1}{2}\{G_{2j-1}(x) + H_{2j-1}(x)\}G_j(x), \tag{2.22}$$

$$H_{3j+1}(x) = \frac{1}{2}\{G_{2j}(x) + H_{2j}(x)\}H_{j+1}(x) - \frac{1}{2}\{G_{2j-1}(x) + H_{2j-1}(x)\}H_j(x). \tag{2.23}$$

Theorem 2.6 (Factorization of polynomials)**.** *For all integers $j \geq 1$, we have*

$$G_j(x) \mid G_{3j+1}(x), \tag{2.24}$$

$$H_j(x) \mid H_{3j+1}(x). \tag{2.25}$$

Proof. Equation (2.8) implies that 2 $G_j(x) \mid \{G_{2j}(x) + H_{2j}\,(x)\}$. From this result and (2.22) we obtain (2.24). Similarly the relation (2.25) follows from (2.8) and (2.23). □

Applying the reduction formulae provided by Theorem 2.5, we obtain the following:

Theorem 2.7. *For all integers $k, j \geq 1$, we have*

$$\begin{aligned} G_{\{(2j+1)k+(3j+1)\}}(x) &= \frac{1}{2}\{G_{2j}(x) + H_{2j}(x)\}G_{\{(2j+1)(k-1)+3j+2\}}(x) \\ &\quad -\frac{1}{2}\{G_{2j-1}(x) + H_{2j-1}(x)\}G_{\{(2j+1)(k-1)+3j+1\}}(x), \end{aligned} \tag{2.26}$$

$$\begin{aligned} H_{\{(2j+1)k+(3j+1)\}}(x) &= \frac{1}{2}\{G_{2j}(x) + H_{2j}(x)\}H_{\{(2j+1)(k-1)+3j+2\}}(x) \\ &\quad -\frac{1}{2}\{G_{2j-1}(x) + H_{2j-1}(x)\}H_{\{(2j+1)(k-1)+3j+1\}}(x). \end{aligned} \tag{2.27}$$

By induction, we have the following theorem.

Theorem 2.8 (Generalized result on the factorization of polynomials)**.** *For $j \in N$ and $k \geq 0$,*

$$G_j(x) \mid G_{\{(2j+1)k+(3j+1)\}}(x), \tag{2.28}$$

$$H_j(x) \mid H_{\{(2j+1)k+(3j+1)\}}(x). \tag{2.29}$$

Theorem 2.9. *It holds that*

$$\gcd\{G_{k-1}(x), G_k(x)\} = 1, \ \forall\, k \geq 1 \tag{2.30}$$

$$\gcd\{G_{k-2}(x), G_k(x)\} = 1, \ \forall\, k \geq 2 \tag{2.31}$$

$$\gcd\{H_{k-1}(x), H_k(x)\} = 1, \ \forall\, k \geq 1 \tag{2.32}$$

$$\gcd\{H_{k-2}(x), H_k(x)\} = 1, \ \forall\, k \geq 2. \tag{2.33}$$

Now we consider the question: Given $j \in N$, which are the polynomials in the $G(x)$-sequence (respectively, $H(x)$-sequence) not divisible by $G_j(x)$ (respectively, $H_j(x)$)? We obtain an important result.

Theorem 2.10. *The following relations hold:* $G_j(x) \nmid G_{j+1}(x), G_{j+2}(x), \ \ldots, \ G_{3j}(x)$ *and* $H_j(x) \nmid H_{j+1}(x), H_{j+2}(x), \ \ldots, \ H_{3j}(x), \forall j \in N$.

Theorem 2.11. *The following properties hold:*

$$G_j(x) \nmid G_{\{(2j+1)k+(3j+1+\lambda)\}}(x), \tag{2.34}$$

$$H_j(x) \nmid H_{\{(2j+1)k+(3j+1+\lambda)\}}(x) \tag{2.35}$$

for all $k \geq 0$ and $\lambda = 1, 2, \ldots, 2j$.

Proof. Assume (2.34) for all positive integers up to λ with $\lambda < 2j+1$. From (2.20) we have

$$\begin{aligned} G_{\{(2j+1)k+(3j+2+\lambda)\}}(x) &= \frac{1}{2}\{G_\lambda(x) + H_\lambda(x)\}G_{\{(2j+1)k+(3j+2)\}}(x) \\ &\quad -\frac{1}{2}\{G_{\lambda-1}(x) + H_{\lambda-1}(x)\}G_{\{(2j+1)k+(3j+1)\}}(x). \end{aligned}$$

The relation (2.28) implies $G_j(x) \mid G_{\{(2j+1)k+(3j+1)\}}(x)$. By induction assumption, it follows that $G_j(x) \nmid G_{\{(2j+1)k+(3j+2)\}}(x)$. Therefore, $G_j(x) \nmid G_{\{(2j+1)k+(3j+2+\lambda)\}}(x)$. This proves (2.34). Similarly one can prove (2.35). □

Divisibility among odd numbers is transformed into an equivalent problem of divisibility among $G(x)$-polynomials or $H(x)$-polynomials as follows:

Theorem 2.12. *The following statements are equivalent:*

(a) $2j+1 \mid 2m+1$,

(b) $G_j(x) \mid G_m(x)$,

(c) $H_j(x) \mid H_m(x), \ \forall\, j, m > 0$.

Proof. Assume (a) holds. Then there exists an odd integer 2s+1 such that

$$2m+1 = (2j+1)(2s+1). \tag{2.36}$$

This relation gives $m = 2js + j + s = (2j+1)(s-1) + (3j+1)$. So m is of the form $(2j+1)k + (2j+1)$ with $k = s-1 \geq 0$. This implies that $G_j(x) \mid G_m(x)$. Thus (a) $\Rightarrow$ (b).

Next, assume (b) holds. Then, by Theorem 2.8, $G_j(x) \mid G_{\{(2j+1)k+(3j+1)\}}(x), \forall k \geq 0$ and by Theorem 2.11, $G_j(x) \nmid G_{\{(2j+1)k+(3j+1+\lambda)\}}(x), \forall k \geq 0$ and $\lambda = 1, 2, ..., 2j$. So $m = (2j+1)k + (3j+1)$ for some integer k. This yields $2m+1 = 4jk + 2k + 6j + 3 = (2j+1)(2s+1)$ with $s = k+1$. Hence $2j+1 \mid 2m+1$. Thus (b) $\Rightarrow$ (a). Similarly we check that (a) $\Leftrightarrow$ (c). □

2.5 Arithmetic progressions

Theorem 2.13. *The sequences $\{G_k(x)\}$ and $\{H_k(x)\}$ of polynomials over $\mathbb{Z}$ contain infinite number of infinite sub-sequences, the subscripts of the terms of which are in arithmetic progression, with non-trivial common factors.*

Example 2.1. *We have $G_1(x) \mid G_4(x), G_7(x), G_{10}(x), \ldots$ and $H_1(x) \mid H_4(x), H_7(x), H_{10}(x), \ldots$. Since $G_1(x) = x - 1$ and $H_1(x) = x + 1$, it is seen that $x - 1 \mid G_j(x)$ and $x + 1 \mid H_j(x)$ for all $j \equiv 1 \pmod 3$.*

Theorem 2.14. *If $2m + 1$ is a prime ≥ 5, then there do not exist $G_j(x)$ and $H_j(x)$ such that $0 < j < m$ and $G_j(x) \mid G_m(x)$ or $H_j(x) \mid H_m(x)$.*

Proof. Suppose $G_j(x) \mid G_m(x)$. Then $2j+1 \mid 2m+1$. Since $2m+1$ is a prime, $2j+1$ is either 1 or $2m+1$. So j is either 0 or m. This implies $G_j(x)$ is 1 or $G_m(x)$, a contradiction. Similar is the case if $H_j(x) \mid H_m(x)$. □

As a consequence of the foregoing discussion, it follows that the only possibilities of the divisors of the polynomials $G_m(x)$ and $H_m(x)$ are as provided by Theorem 2.12.

2.6 Products and quotients of polynomials

Theorem 2.15. *If $G_i(x)$ and $G_j(x) \in \{G_k(x)\}$, then $G_i(x)G_j(x) \notin \{G_k(x)\}$. If $H_i(x)$ and $H_j(x) \in \{H_k(x)\}$, then $H_i(x)H_j(x) \notin \{H_k(x)\}$.*

Proof. The leading coefficient and the coefficient of x^{k-1} in $G_k(x)$ are 1 and -1, respectively. The coefficient of x^{i+j-1} in $G_i(x)G_j(x)$ is -2. Consequently $G_i(x)G_j(x) \notin \{G_k(x)\}$. The leading coefficient and the coefficient of x^{k-1} in $H_k(x)$ are both 1. The coefficient of x^{i+j-1} in $H_i(x)H_j(x)$ is 2. Therefore, $H_i(x)H_j(x) \notin H_k(x)\}$. □

For $j \in N$ and $k \geq 0$, by Theorem 2.8 we have $G_j(x) \mid G_{\{(2j+1)k+(3j+1)\}}(x)$ and $H_j(x) \mid H_{\{(2j+1)k+(3j+1)\}}(x)$. As a consequence of Theorem 2.15, we obtain the following result:

Theorem 2.16. *The quotient polynomials $\frac{G_{(2j+1)k+3j+1(x)}}{G_j(x)}$ and $\frac{H_{(2j+1)k+3j+1}(x)}{H_j(x)} \notin \{G_k(x)\}$ and $\{H_k(x)\}$, respectively.*

2.7 Satellite polynomials

Let us consider $G_m(x)$ and $H_m(x)$, where $2m+1$ is a composite number. The result contained in Theorem 2.16 leads to the following.

Definition 2.4 (Satellite polynomial)**.** *A polynomial $p(x) \in \mathbb{Z}[x]$ is said to be a satellite polynomial for $G_j(x)$ if $p(x) \mid G_j(x)$ but $p(x) \notin \{G_k(x)\}$. A polynomial $q(x) \in \mathbb{Z}[x]$ is said to be a satellite polynomial for $H_j(x)$ if $q(x) \mid H_j(x)$ but $q(x) \notin \{H_k(x)\}$.*

Example 2.2. *The polynomial $p(x) = x^3 - 3x - 1 \mid G_4(x)$ but $p(x) \notin \{G_k(x)\}$. Therefore $p(x)$ is a satellite polynomial f or $G_4(x)$.*
The polynomial $q(x) = x^3 - 3x + 1 \mid H_4(x)$ but $q(x) \notin \{H_k(x)\}$. Therefore $q(x)$ is a satellite polynomial for $H_4(x)$.

As a consequence of Theorems 2.12 and 2.16, we have

Theorem 2.17. *When $2m+1$ is composite, $G_m(x)$ (respectively, $H_m(x)$) is a product of at least one polynomial in $\{G_k(x)\}$ (resp. $\{H_k(x)\}$) and at least one satellite polynomial.*

3 The M-sequences and cycles in the field $\mathbb{F}_\rho$

The polynomial sequences $\{F_k(x)\}$, $\{G_k(x)\}$ and $\{H_k(x)\}$ in $\mathbb{Z}[x]$ have been introduced in Section 2. It would be worthwhile to determine the interplay among the values assumed by these sequences in a finite field. We deal with the first sequence in this section and the other two sequences will be taken up in the next section.

Definition 3.1 (The sequence $\{M_k\}$ in $\mathbb{F}_\rho$)**.** *Let ρ be given odd prime. Consider the field $\mathbb{F}_\rho = \{0,\ 1, \ldots, \rho - 1\}$. Choose any element $M \in \mathbb{F}_\rho$ and fix it. Define the infinite sequence $\{M_k\}$ in $\mathbb{F}_\rho$ as follows:*

$$M_k = F_k(M)\ (k \geq 1), \tag{3.1}$$

where F is defined by (2.1) *and each M_k is reduced modulo ρ.*

We have $M_1 = M, M_2 = M^2 - 2, M_3 = M^4 - 4M^2 + 2$, etc. Thus the terms of the sequence $\{M_k\}$ are polynomial expressions in M with coefficients from $\mathbb{F}_\rho$. The sequence $\{M_k\}$ will be referred to as the M-sequence in $\mathbb{F}_\rho$.

Definition 3.2 (Stationary M-sequences in $\mathbb{F}_\rho$)**.** *We call the two sequences $2 \to 2 \to 2 \to \cdots$ and $-1 \to -1 \to -1 \to \cdots$ as stationary M-sequences in $\mathbb{F}_\rho$.*

In the case of $\rho = 3$, the two sequences become identical. Let us assume $\rho > 3$ so that the two sequences are distinct.

Definition 3.3 (Singular and non-singular sequences)**.** *We refer to the sequence $2 \to 2 \to 2 \to \cdots$ as singular and the sequence $-1 \to -1 \to -1 \to \cdots$ as non-singular in $\mathbb{F}_\rho$.*

This terminology is used in the sense that the latter sequence possesses a property in common with some other non-stationary M-sequence in $\mathbb{F}_\rho$ as would be seen in the course of subsequent development of the theory.

If we start with $M = 0, 2$ or -2, we end up with the stationary M-sequence $2 \to 2 \to 2 \to \cdots$. If we take $M = 1$ or -1, we obtain the stationary M-sequence $-1 \to -1 \to -1 \to \cdots$.

Hence, in order to obtain non-stationary M-sequences in $\mathbb{F}_\rho$, we have to exclude the values $M = 0, \pm 1, \pm 2$. Suppose $M \in \mathbb{F}_\rho$ such that $M \neq 0, \pm 1, \pm 2$. If $M^2 = 2$, then we get the stationary M-sequence $M \to 0 \to -2 \to -2 \to -2 \to \cdots$ and if $M^2 = 3$, then there results the stationary M-sequence $M \to 1 \to -1 \to -1 \to -1 \to \cdots$. So, a necessary condition for getting a non-stationary M-sequence in $\mathbb{F}_\rho$ is that $M \neq 0, \pm 1, \pm 2$ and $M^2 \neq 2, 3$. However, the restrictions $M \neq 0, \pm 1, \pm 2$ and $M^2 \neq 2, 3$ are not sufficient to produce a non-stationary M-sequence in $\mathbb{F}_\rho$ as illustrated by the following.

Example 3.1. *For $\rho = 17$ and $M = 5$, we get the sequence $5 \to 6 \to 0 \to -2 \to 2 \to 2 \to \cdots$.*

Theorem 3.1 (Necessary and sufficient condition)**.** *Given $M \in \mathbb{F}_\rho$, let M_k be a general term of the M-sequence in $\mathbb{F}_\rho$. A necessary and sufficient condition for the M-sequence to be non-stationary is that $M \neq 0, \pm 1, \pm 2$ and $M_k^2 \neq 2, 3, \ \forall\ k \in N$.*

Proof. We establish the sufficiency of the condition. Assume that $M \neq 0, \pm 1, \pm 2$ and $M_k^2 \neq 2, 3, \forall k \in N$. These conditions imply that $M_2 = M_1^2 - 2 \neq 0, \pm 1, \pm 2$. Similarly we check that $M_k \neq 0, \pm 1, \pm 2, \forall\ k \geq 3$. Hence the M-sequence is non-stationary. □

Restriction on ρ: The conditions $M \neq 0, \pm 1, \pm 2$ and $M_k^2 \neq 2, 3, \forall\ k \in N$, imply that we have to choose $\rho \geq 11$, in order to obtain a non-stationary M-sequence in $\mathbb{F}_\rho$.

Notation: Let $(\frac{p}{q})$ denote the Jacobi symbol. In view of Theorem 3.1, if either of $(\frac{2}{\rho})$, $(\frac{3}{\rho})$ is $+1$, then we have to exclude $M \in \mathbb{F}_\rho$ with the property $M^2 = 2$ or 3, so as to get a non-stationary M-sequence.

Theorem 3.2. *If $M \in \mathbb{F}_\rho - \{0, \pm 1, \pm 2\}$ and $M^2 \notin \{2, 3\}$, then M_2 is different from both M_1 and M_3.*

Proof. Clearly, $M_2 \neq 0, \pm 1, \pm 2$. If $M_2 = M_1$, then we have $M - 2 = M$. i.e., $(M + 1)(M - 2) = 0$. This implies that $M = -1$ or 2, which is a contradiction. Hence $M_2 \neq M_1$. Next, if $M_2 = M_3$, then we must have $M^4 - 4M^2 + 2 = M^2 - 2$. i.e., $(M^2 - 1)(M^2 - 4) = 0$. This implies that $M = \pm 1, \pm 2$, again a contradiction. So $M_2 \neq M_3$. □

Definition 3.4 (Cycle-contributing element)**.** *An element $M \in \mathbb{F}_\rho$ is said to be a cycle-contributing element if the sequence $\{M_k \pmod \rho\}$ contains a cycle as follows: $M = M_1 \to M_2 \to \cdots \to M_j \to M_{j+1} \to \cdots \to M_j \to \cdots$, where $M_{j+1} \neq M_j$ for some $j \in N$.*

Definition 3.5 (Cycle-forming element)**.** *An element $M \in \mathbb{F}_\rho$ is said to be a cycle-forming element if the sequence $\{M_k \pmod \rho\}$ contains a cycle as follows: $M = M_1 \to M_2 \to M_3 \to \cdots \to M_1 \to \cdots$, where $M_2 \neq M_1$.*

Definition 3.6 (In-cycle element)**.** *A cycle-forming element in $\mathbb{F}_\rho$ is called an in-cycle element.*

Definition 3.7 (Ex-cycle element)**.** *A cycle-contributing element but not cycle-forming element in $\mathbb{F}_\rho$ is called an ex-cycle element.*

Theorem 3.3. *If M is an in-cycle or ex-cycle element in $\mathbb{F}_\rho$, then $-M$ is an ex-cycle element.*

Definition 3.8 (M-cycle)**.** *If M is an in-cycle element in $\mathbb{F}_\rho$, then a cycle beginning with M and ending with M is called an M-cycle and the numbers in the cycle are called its elements.*

Definition 3.9 (Background prime). *If M is an in-cycle element in $\mathbb{F}_\rho$, we refer to ρ as the background prime for the M-cycle.*

Definition 3.10 (Length of an $M-$cycle). *Consider an M-sequence $(\mathrm{mod}\ \rho)$ containing a cycle $M = M_1 \to M_2 \to \cdots \to M_j \to M_{j+1} \to \cdots$. If n is the smallest natural number such that $M_{n+1} = M_1$ then we say that the M-sequence has period n and the cycle has length n.*

The following result lays the foundation for the major results in the later sections.

Theorem 3.4 (Existence of M-cycle in $\mathbb{F}_\rho$). *If ρ is an odd prime ≥ 11, then there exists at least one M-cycle of length ≥ 2 in $\mathbb{F}_\rho$.*

Proof. We provide a construction proof. First consider the case when $(\frac{2}{\rho}) = +1$ and $(\frac{3}{\rho}) = +1$. Working backwards with the sequence $2 \to 2 \to 2 \to \cdots$, consider the predecessor elements. There exist elements $a_1, a_2, \ldots, a_r \in \mathbb{F}_\rho$ such that $a_1 \to a_2 \to \cdots \to a_r \to a_{r+1} = 0 \to a_{r+2} = 2 \to 2 \to 2 \to \cdots$ for some index r. This implies that $a_r^2 \equiv 2(\mathrm{mod}\ \rho)$. Since $a_r = a_{r-1}^2 - 2$, it follows that $a_r + 2$ is expressible as a square in $\mathbb{F}_\rho$. Similarly, each one of $a_{r-1}+2, a_{r-2}+2, \ldots, a_1+2$ is a quadratic residue modulo ρ. However, since there exist quadratic non-residues modulo ρ, the predecessor elements in the above sequence cannot exhaust all the elements of $\mathbb{F}_\rho$. A similar observation applies to the sequence $-1 \to -1 \to -1 \to \cdots$. Take an element $b_1 \in \mathbb{F}_\rho$, not exhausted by the predecessor elements of the two stationary sequences in $\mathbb{F}_\rho$. Then $b_1 \not\equiv 0, \pm 1, \pm 2$ and $b_1^2 \not\equiv 2, 3\ (\mathrm{mod}\ \rho)$. Consider the sequence $b_1 \to b_2 \to b_3 \to \cdots \to b_{k-1} \to b_k \to \cdots$, where $b_k = b_{k-1}^2 - 2$, for all $k \geq 2$. We check that $b_k^2 \not\equiv 2, 3\ (mod\ \rho)$ for all $k \geq 2$. By Theorem 3.2, $b_2 \neq b_1$ and $b_2 \neq b_3$. Since $\mathbb{F}_\rho$ has exactly ρ elements, it follows that there exist integers $k \neq j$ such that $b_k = b_j$. Thus the above sequence is non-stationary and it contains a cycle of length ≥ 2. A similar proof applies when only one or none of $(\frac{2}{\rho})$, $(\frac{3}{\rho})$ is $+1$. □

Theorem 3.5 (Uniqueness of M-cycle and its length in $\mathbb{F}_\rho$). *For an M-cycle element in $\mathbb{F}_\rho$,*

(i) the M-cycle in which it occurs is unique.

(ii) the length of the M-cycle in which it occurs is unique.

4 The sequences $\{\theta_{t,k}\}$ and $\{\psi_{t,k}\}$ in the field $\mathbb{F}_\rho$

In this section, we introduce two sequences in the field $\mathbb{F}_\rho$ and establish their properties.

4.1 M-cycle through a parameter

Let ρ be a given odd prime ≥ 11. In order to identify the relationship that an M-cycle has with the values assumed by the sequences $\{G_k(x)\}$ and $\{H_k(x)\}$ in $\mathbb{F}_\rho$, the introduction of a parameter becomes necessary. We consider a non-stationary M-cycle in $\mathbb{F}_\rho$ attached with a parameter t. Choose any in-cycle element $M(t) \in \mathbb{F}_\rho$. Then $M(t) \neq 0, \pm 1, \pm 2$. By our assumption, the resulting cycle in $\mathbb{F}_\rho$ has a period $n \geq 2$. Denote the cycle by $M_1 \to M_2 \to \cdots \to M_n \to M_{n+1} = M_1 \to \cdots$, where $M_1 = M(t), M_2 = M(t+1) = M_1^2 - 2, \ldots, M_n = M(t+n-1) = M_{n-1}^2 - 2$ and

$$M_{n+1} = M(t+n) = M_n^2 - 2 = M(t) = M_1. \tag{4.1}$$

Example 4.1. *Consider* $\rho = 65537$. *We see that* $(\frac{989}{65537}) = 1$. *On computation, we obtain* $1355^2 = 1836025 \equiv 989 \pmod{65537}$. *Hence* $1355^2 - 2 \equiv 987 \pmod{65537}$. *Choosing* $M_1 = M(t) = 987$, *we get the cycle* $M(t) \to M(t+1) \to \cdots \to M(t+14) \to M(t+15) = M(t)$ *in the field* $\mathbb{F}_\rho$ *with the explicit expression* $987 \to 56649 \to 24457 \to 54185 \to 22160 \to 62394 \to 47897 \to 65459 \to 6082 \to 27854 \to 18308 \to 26644 \to 5950 \to 12518 \to 1355 \to 987 \to \cdots$

Definition 4.1 (The sequences $\{\theta_{t,k}\}, \{\psi_{t,k}\}$)**.** *Define the infinite sequences* $\{\theta_{t,k}\}$ *and* $\{\psi_{t,k}\}$ $(k \geq 0)$ *in* $\mathbb{F}_\rho$ *as follows:*

$$\left.\begin{array}{l} \theta_{t,k} = \text{ the least non-negative residue of } G_k\,(M(t)) \pmod{\rho} \\ \psi_{t,k} = \text{ the least non-negative residue of } H_k\,(M(t)) \pmod{\rho} \end{array}\right\} \tag{4.2}$$

where G *and* H *are defined by* (2.2), (2.3) *or* (2.4). *Considering* (2.5), *we define the matrix* $\mathfrak{a}(M(t))$ *with elements from* $\mathbb{F}_\rho$ *as follows:*

$$\mathfrak{a}(M(t)) = \begin{bmatrix} \theta_{t,0} & \theta_{t,1} & \theta_{t,2} & \cdots \\ \psi_{t,0} & \psi_{t,1} & \psi_{t,2} & \cdots \end{bmatrix} \tag{4.3}$$

4.2 Cyclic nature of the sequence $\{\theta_{t,k}\}$

To establish the cyclic nature of the $\theta_{t,k}$-sequence, we require a relationship between $M(t)$ and $M(t-1)$ through the terms of the $\theta_{t,k}$-sequence. This crucial relationship is presented below.

Theorem 4.1. *The following relation holds in* $\mathbb{F}_\rho$*:*

$$M(t)\theta_{t+1,k} = \{M(t-1)\}^2\,\theta_{t,k}^2 - 2,\ \forall\, k \geq 0. \tag{4.4}$$

Proof. The relation (4.4) holds for $k = 0$. Assume (4.4) for all positive integers up to k. In view of (2.11), we have $\{\theta_{t,k-1}\}^2 + \{\theta_{t,k}\}^2 = M(t)\theta_{t,k-1}\theta_{t,k} - M(t) + 2$. Using $M(t) - 2 = \{M(t-1)\}^2 - 4$ in the above relation, we obtain $\{\theta_{t,k-1}\}^2 + \{\theta_{t,k}\}^2 + \{M(t-1)\}^2 - 4 = M(t)\theta_{t,k-1}\theta_{t,k}$.

Multiplying both sides by $2\{M(t-1)\}^2$ and using the relation

$$\{M(t)\}^2 = \{M(t-1)\}^4 - 4\{M(t-1)\}^2 + 4,$$

we get

$$2\{M(t-1)\}^2\{\theta_{t,k-1}\}^2 + 2\{M(t-1)\}^2\{\theta_{t,k}\}^2 + 2\{M(t)\}^2 = 2\{M(t-1)\}^2 M(t)\theta_{t,k-1}\theta_{t,k} + 8.$$

Adding $\{M(t-1)\ M(t)\theta_{t,k}\}^2$ to both sides, we get

$$\begin{aligned} &\{M(t-1)\}^2\{(M(t))^2(\theta_{t,k})^2 - 2M(t)\theta_{t,k-1}\theta_{t,k} + (\theta_{t,k-1})^2\} - 2 \\ &= \{M(t-1)\}^2\{(\,M(t))^2 - 2\}\{\theta_{t,k}\}^2 - \{M(t-1)\}^2\,(\theta_{t,k-1})^2 - 2\{(\,M(t))^2 - 2\} + 2. \end{aligned}$$

Using induction assumption, we obtain

$$\begin{aligned} &\{M(t-1)\}^2\{M(t)\theta_{t,k} - \theta_{t,k-1}\}^2 - 2 \\ &= M(t+1)\{M(t)\theta_{t+1,k} + 2\} - \{M(t)\theta_{t+1,k-1} + 2\} - 2M(t+1) + 2 \\ &= M(t)\{M(t+1)\theta_{t+1,k} - \theta_{t+1,k-1}\}, \end{aligned}$$

i.e., $\{M(t-1)\}^2\{\theta_{t,k+1}\}^2 - 2 = M(t)\theta_{t+1,k+1}$.
Hence the relation (4.4) follows by induction on k. □

In order to derive the properties of the $M(t)$-cycles, we need two important transformations. The first to be introduced is the following.

Definition 4.2 (The transformation τ_t)**.** *With respect to the $M(t)$-cycle under consideration, define $\tau_t : \mathbb{F}_\rho \to \mathbb{F}_\rho$ by the rule*

$$\tau_t(\alpha) = \frac{M(t-1)^2\alpha^2 - 2}{M(t)} \tag{4.5}$$

$\forall\ \alpha \in \mathbb{F}_\rho$, *where* $\frac{1}{M(t)}$ *is the multiplicative inverse of* $M(t)$ *in* $\mathbb{F}_\rho$.

Theorem 4.2 (Cyclic nature of $\theta_{t,k}$ as a function of t)**.** *The following relation holds for all* $k \geq 0$:

$$\tau_t(\theta_{t,k}) = \theta_{t+1,k}. \tag{4.6}$$

Proof. Follows from the relation (4.4). □

Corresponding to the cycle $M(t) = M_1\ rightarrow M_2 \to \cdots \to M_n \to M_{n+1} = M_1$ in $\mathbb{F}_\rho$, we obtain the cycle $\theta_{t,j} \to \theta_{t+1,j} \to \cdots \to \theta_{t+n-1,j} \to \theta_{t+n,j} = \theta_{t,j},\ \forall\ j \geq 0$.

Theorem 4.3. *The* $\{\theta_{t,k} \pmod{\rho}\}$*-sequence never attains the value of* 0 *or* -1.

Proof. If possible, suppose that there exists a natural number j such that $\theta_{t,j} = 0$. Using Theorem 4.2 successively, we get

$$\theta_{t+1,j} = -\frac{2}{M(t)}, \theta_{t+2,j} = \frac{2}{M(t+1)}, \ldots,\ \theta_{t+n,j} = \frac{2}{M(t+n-1)}.$$

So the cycle $\theta_{t,j} \to \theta_{t+1,j} \to \cdots \to \theta_{t+n,j}$ becomes $0 \to -\frac{2}{M(t)} \to \frac{2}{M(t+1)} \to \cdots \to \frac{2}{M(t+n-1)}$. However, $\frac{2}{M(t+n-1)} \neq 0$. Therefore, $\theta_{t+n,j} \neq \theta_{t,j}$, which is a contradiction.

Consequently, $\theta_{t,j} \neq 0, \forall j \geq 0$. Next, suppose that there exists some $s \in N$ such that $\theta_{t,s} = -1$. Then the cycle $\theta_{t,s} \to \theta_{t+1,s} \to \cdots \to \theta_{t+n,s}$ becomes $-1 \to 1 \to 1 \to \cdots \to 1$. This implies that $\theta_{t+n,s} \neq \theta_{t,s}$, which is a contradiction. The proof is now complete. □

4.3 Cyclic nature of $\{\psi_{t,k}\}$-sequence as a function of t

Theorem 4.4. *The following relation holds:*

$$\theta_{t,k}\psi_{t,k} = \psi_{t+1,k},\ \forall\ k \geq 0. \tag{4.7}$$

Proof. The result is true for $k = 0$. Assume (4.7) for all integers up to k. Using (2.3) and (2.4) we obtain $\theta_{t,k+1}\psi_{t,k+1} = \{M(t)\theta_{t,k} - \theta_{t,k-1}\}\{M(t)\psi_{t,k} - \psi_{t,k-1}\}$. In view of the relation (2.13), we get

$$\begin{aligned}\theta_{t,k+1}\psi_{t,k+1} &= \{M(t)\}^2\theta_{t,k}\psi_{t,k} - 2(\theta_{t,k-1}\psi_{t,k-1} + \theta_{t,k}\psi_{t,k}) + \theta_{t,k-1}\psi_{t,k-1} \\ &= \{M(t)^2 - 2\}\theta_{t,k}\psi_{t,k} - \theta_{t,k-1}\psi_{t,k-1}.\end{aligned}$$

Using induction hypothesis, we obtain $\theta_{t,k+1}\psi_{t,k+1} = M(t+1)\psi_{t+1,k} - \psi_{t+1,k-1}$. Because of the relation (2.3), we get $\theta_{t,k+1}\psi_{t,k+1} = \psi_{t+1,k+1}$. Hence (4.7) holds by induction on k. □

The second tool required is the following.

Definition 4.3 (The transformation σ_t)**.** *Define* $\sigma_t : \mathbb{F}_\rho \times \mathbb{F}_\rho \to \mathbb{F}_\rho$ *by the rule*

$$\sigma_t(\alpha, \beta) = \alpha\beta, \ \forall \ \alpha, \beta \in \mathbb{F}_\rho. \tag{4.8}$$

Theorem 4.5. *The following property holds:*

$$\sigma_t(\theta_{t,k}, \psi_{t,k}) = \psi_{t+1,k}, \forall \ k \geq \ 0. \tag{4.9}$$

Proof. Follows from the relation (4.7). □

Corresponding to the cycle $M(t) = M_1 \to M_2 \to \cdots \to M_n \to M_{n+1} = M_1$ in $\mathbb{F}_\rho$, we obtain the cycle $\psi_{t,j} \to \psi_{t+1,j} \to \cdots \to \psi_{t+n-1,j} \to \psi_{t+n,j} = \psi_{t,j}, \forall \ j \geq 0$.

Theorem 4.6. *Let* t *be varying. For each fixed* k*, the cyclic sequences* $\{\theta_{t,k} \pmod \rho\}$ *and* $\{\psi_{t,k} \pmod \rho\}$ *as functions of* t *are periodic with the same period as that of the cycle* $M_1 \to M_2 \to \cdots \to M_n \to M_{n+1} = M_1$.

Proof. Follows from the relations (2.3), (2.4), (4.1), (4.6) and (4.9). □

Example 4.2. *Consider* $\rho = 26879$. *We have* $(\frac{12935}{26879}) = 1$. *Take* $M_1 = M(t) = 12933$. *We have the* M*-cycle* $12933 \to 21349 \to 19475 \to 12933 \to \cdots$ *with period* 3. *Next take* $M_2 = 21349$ *and* $M_3 = 19475$. *Corresponding to* M_i $(i = 1, 2, 3)$*, we construct Table 4.1 consisting of the terms of the sequences* $\theta_{t,k}$ *and* $\psi_{t,k} \pmod{26879}$*, using* (2.2) *or equivalently* (2.3) *and* (2.4)*. The table consists of three parts contributed by the values of* $M_i's$.

Table 4.1. M-cycles in $\mathbb{F}_{26879}$

k	0	1	2	3	4	5	6	7	8	$\cdots$
$\theta_{t,k}$	1	12932	8417	11058	8417	12932	1	1	12932	$\cdots$
$\psi_{t,k}$	1	12934	7404	0	19475	13945	26878	1	12934	$\cdots$
k	0	1	2	3	4	5	6	7	8	$\cdots$
$\theta_{t,k}$	1	21348	25006	14806	25006	21348	1	1	21348	$\cdots$
$\psi_{t,k}$	1	21350	13946	0	12933	5529	26878	1	21350	$\cdots$
k	0	1	2	3	4	5	6	7	8	$\cdots$
$\theta_{t,k}$	1	19474	20338	1011	20338	19474	1	1	19474	$\cdots$
$\psi_{t,k}$	1	19476	5530	0	21349	7403	26878	1	19476	$\cdots$

As a consequence of the cyclic nature of $\theta_{t,k}$ *and* $\psi_{t,k}$ *as functions of* t*, starting with any one part of the above table, we can construct the other two parts of the table.*

5 Structure of $\{\theta_{t,k}\}$ and $\{\psi_{t,k}\}$-sequences in the field $\mathbb{F}_\rho$

In this section, we exhibit how the $\theta_{t,k}$ and $\psi_{t,k}$-sequences, considered as functions of t, can be split into several identical parts and determine the structure of such parts in $\mathbb{F}_\rho$.

Definition 5.1. *(Neighboring elements and neighboring region). Let t be fixed. For $\theta_{t,k}$ (respectively, $\psi_{t,k}$), we say that the neighboring elements are $\theta_{t,k-1}$ and $\theta_{t,k+1}$ (respectively, $\Psi_{t,k-1}$ and $\psi_{t,k}$). For given t, any three consecutive elements in the $\theta_{t,k}$ (respectively, $\psi_{t,k}$)-sequence constitute a neighboring region with respect to the middle element among them.*

5.1 Properties of the neighboring elements in $\{\theta_{t,k}(\mathrm{mod}\ \rho)\}$ and $\{\psi_{t,k}(\mathrm{mod}\ \rho)\}$-sequences

Theorem 5.1. *If the relation*

$$\theta_{t,j} = \theta_{t,j+1}\,(\mathrm{mod}\ \ \rho) \tag{5.1}$$

holds for some integer j, then

$$\theta_{t,j} = 1 \textit{ and } \psi_{t,j+1} = \psi_{t,j} + 2\ (\mathrm{mod}\ \rho). \tag{5.2}$$

Proof. Suppose (5.1) holds for some integer j. Using Theorem 2.2 and the relation (5.1) we have $\theta_{t,j}(\psi_{t,j+1} - \psi_{t,j}) = 2$. In view of the relation (2.6), we obtain $\psi_{t,j+1} = \psi_{t,j} + 2\theta_{t,j}$. Consequently we get

$$\theta_{t,j} = \pm 1. \tag{5.3}$$

However, by Theorem 4.4, the $-$ sign cannot hold in (5.3). So $\psi_{t,j+1} = \psi_{t,j} + 2$. □

Corollary 5.1. *There does not exist an integer j such that*

$$\theta_{t,j} = \theta_{t,j+1}\ (\mathrm{mod}\ \rho) \textit{ and } \psi_{t,j} = \psi_{t,j+1}\ (\mathrm{mod}\ \rho).$$

Theorem 5.2. *If the relation*

$$\theta_{t,j} = \psi_{t,j}\,(\mathrm{mod}\ \rho) \tag{5.4}$$

holds for some positive integer j, then $\theta_{t,j} = 1,\ \theta_{t,j-1} = 1$ and $\psi_{t,j-1} = -1$.

Proof. Assume (5.4) holds for some $j > 0$. Then, because of the relation (2.6), we have $\psi_{t,j+1} = 2\theta_{t,j} + \theta_{t,j+1}$. In view of Theorem 2.2, we obtain $\theta_{t,j}^2 = 1$. This implies that

$$\theta_{t,j-1} - \psi_{t,j-1} = 2. \tag{5.5}$$

However, in view of Theorem 2.1 we have

$$\theta_{t,j-1} + \psi_{t,j-1} = \psi_{t,j} - \theta_{t,j} = 0. \tag{5.6}$$

Solving the equations (5.5) and (5.6), we obtain $\theta_{t,j-1} = 1$ and $\psi_{t,j-1} = -1$. □

5.2 Method of finding successor and predecessor elements

We consider the forward movement in $\{\theta_{t,k}\ (\mathrm{mod}\ \ \rho)\}$ and $\{\psi_{t,k}\ (\mathrm{mod}\ \ \rho)\}$-sequences. i.e., $\theta_{t,r} \to \theta_{t,r+1} \to \cdots$ and $\psi_{t,r} \to \psi_{t,r+1} \to \cdots (\mathrm{mod}\ \rho)$. We obtain the formulae

$$\theta_{t,r+1} = \frac{(\psi_{t,r} + \theta_{t,r})\theta_{t,r} - 2}{\psi_{t,r} - \theta_{t,r}}. \tag{5.7}$$

and

$$\psi_{t,r+1} = \frac{(\psi_{t,r} + \theta_{t,r})\psi_{t,r} - 2}{\psi_{t,r} - \theta_{t,r}},\ \text{provided } \theta_{t,r} \not\equiv \psi_{t,r}\ (\mathrm{mod}\ \rho). \tag{5.8}$$

Next we consider the backward movement in $\{\theta_{t,k} \pmod{\rho}\}$ and $\{\psi_{t,k} \pmod{\rho}\}$-sequences. i.e., $\cdots \leftarrow \theta_{t,r-1} \leftarrow \theta_{t,r}$ and $\cdots \leftarrow \psi_{t,r-1} \leftarrow \psi_{t,r} \pmod{\rho}$. We have

$$\theta_{t,r-1} = \frac{(\psi_{t,r} - \theta_{t,r})\theta_{t,r} + 2}{\theta_{t,r} + \psi_{t,r}} \tag{5.9}$$

and

$$\psi_{t,r-1} = \frac{(\psi_{t,r} - \theta_{t,r})\psi_{t,r} - 2}{\theta_{t,r} + \psi_{t,r}}, \text{ provided } \theta_{t,r} + \psi_{t,r} \not\equiv 0 \pmod{\rho}. \tag{5.10}$$

5.3 Symmetric and skew-symmetric properties

Definition 5.2 (Subsets of a sequence with symmetric or skew-symmetric property)**.** *Consider two distinct sets with the same cardinality consisting of consecutive elements from a sequence* $\{S_n\} \pmod{\rho}$. *Let them be* $\{S_k, S_{k+1}, \ldots, S_{k+r-1}\}$ *and* $\{S_{h-r+1}, \ldots, S_{h-1}, S_h\}$. *We impose the condition* $h \geq k + 2r - 2$ *so that the first set can be referred to as the set in the left side and the second set can be referred to as the set in the right side. We say that the two sets possess symmetric property if*

$$S_k = S_h,\ S_{k+1} = S_{h-1}, \ldots S_{k+r-1} = S_{h-r+1}. \tag{5.11}$$

We say that the two sets have skew-symmetric property if

$$S_k = -S_h,\ S_{k+1} = -S_{h-1},\ S_{k+r-1} = -S_{h-r+1.} \tag{5.12}$$

Using (2.3) and (2.4) we obtain the following theorem.

Theorem 5.3 (Extension of symmetric and skew-symmetric sets)**.** *Suppose there are two distinct pairs of consecutive elements in* $\{\theta_{t,k} \pmod{\rho}\}$*-sequence with symmetric property. Suppose the elements in the corresponding positions of* $\{\psi_{t,k} \pmod{\rho}\}$*-sequence possess skew-symmetric property. Then the cardinalities of these sets can be increased by* 1*, still maintaining the symmetric and skew-symmetric properties of the respective sets, with the inclusion of the successor elements in the forward movements of the left side sets and the predecessor elements in the backward movements of the right side sets.*

By induction, we have the following corollary.

Corollary 5.2. *Under the assumptions of Theorem 5.3, the cardinalities of the left side sets and the right side sets can be increased by any desired natural number, still maintaining the symmetric and skew-symmetric properties of the respective sets, with the inclusion of the successor elements in the forward movements of the left side sets and the predecessor elements in the backward movements of the right side sets.*

5.4 Existence of identical parts

Because of the finiteness of $\mathbb{F}_\rho$, there exist two positive integers $r > j$ such that

$$\theta_{t,r} = \theta_{t,j} \text{ and } \psi_{t,r} = \psi_{t,j}. \tag{5.13}$$

Without loss of generality, we may assume that r is the smallest positive integer $> j$ satisfying (5.13). Modulo ρ, we see that $\theta_{t,j} + \psi_{t,j}$ and $-\theta_{t,j}$ cannot both be 0 simultaneously. So we can apply either (5.7), (5.8) or (5.9), (5.10).

With forward and backward movements around $\theta_{t,j}$ and $\psi_{t,j}$, one obtains the elements in the $\{\theta_{t,k} \pmod{\rho}\}$ and $\{\psi_{t,k} \pmod{\rho}\}$-sequences as in (5.14)

$$\begin{bmatrix} \dots & 1 & 1 & \cdots & \theta_{t,j-1}\ \theta_{t,j}\ \theta_{t,j+1} & \dots & 1 & 1 & \cdots \\ \cdots & -1 & 1 & \dots & \psi_{t,j-1}\ \psi_{t,j}\ \psi_{t,j+1} & \cdots & -1 & 1 & \cdots \end{bmatrix} \tag{5.14}$$

Similarly movements around $\theta_{t,r}$ and $\psi_{t,r}$ yield the elements in the $\{\theta_{t,k} \pmod{\rho}\}$ and $\{\psi_{t,k} \pmod{\rho}\}$-sequences as in (5.15):

$$\begin{bmatrix} \cdots & 1 & 1 & \dots & \theta_{t,r-1}\ \theta_{t,r}\ \theta_{t,r+1} & \cdots & 1 & 1 & \cdots \\ \cdots & -1 & 1 & \cdots & \psi_{t,r-1}\ \psi_{t,r}\ \psi_{t,r+1} & \cdots & -1 & 1 & \dots \end{bmatrix} \tag{5.15}$$

The minimality of r implies that the sub-matrix $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ of $\mathfrak{a}(M(t))$ succeeding the elements $\theta_{t,j}$ and $\psi_{t,j}$ cannot be the one other than the sub-matrix $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ of $\mathfrak{a}(M(t))$ preceding the elements $\theta_{t,r}$ and $\psi_{t,r.}$ The elements have the property $\theta_{t,j-1} = \theta_{t,r-1},\ \psi_{t,j-1} = \psi_{t,r-1},\ \theta_{t,j} = \theta_{t,r},$ $\psi_{t,j} = \psi_{t,r}$ and $\theta_{t,j+1} = \theta_{t,r+1},, \psi_{t,j+1} = \psi_{t,r+1.}$ Applying the forward and backward movements around $\theta_{t,j},\ \psi_{t,j}, \theta_{t,r},\ \psi_{t,r}$, we see that each sequence contains two identical parts constituted by the elements in (5.14) and (5.15).

Definition 5.3 (Compartments of $\mathfrak{a}(M(t))$)**.** *The sub-matrix with* 2 *rows of* $\mathfrak{a}(M(t))$*, starting with* 1 *and ending with the next immediate* 1 *in the* $\theta_{t,k} \pmod{\rho}$*-sequence and starting with* 1 *and terminating with the next immediate* $-$ *1 in the* $\psi_{t,k} \pmod{\rho}$*-sequence is called a compartment of the matrix* $\mathfrak{a}(M(t))$*. Given* t*, it follows that any two compartments in* $\mathfrak{a}(M(t))$ *have the same number of elements in the* $\theta_{t,k}$*-sequence as well as the* $\psi_{t,k}$*-sequence. Let* $\mathfrak{C}_1(t)$ *denote the first compartment of* $\mathfrak{a}(M(t))$*. We call* $\mathfrak{C}_1(t)$ *the principal compartment in* $\mathfrak{a}(M(t))$*.*

Theorem 5.4 (Nature of the compartment $\mathfrak{C}_1(t)$)**.** *Given* t*, the number of elements of* $\theta_{t,k}$ *and* $\psi_{t,k}$*-sequences in the compartment* $\mathfrak{C}_1(t)$ *cannot be even.*

5.5 Existence of symmetric and skew-symmetric properties

An important characteristic of the $\theta_{t,k} \pmod{\rho}$-sequence is the symmetric property while that of the $\psi_{t,k} \pmod{\rho}$-sequence is the skew-symmetric property, as established in the sequel. For a given t, it follows from Theorem 5.4 that the number of elements in $\mathfrak{C}_1(t)$ of $\theta_{t,k} \pmod{\rho}$ as well as $\psi_{t,k} \pmod{\rho}$-sequences is odd. We denote this number by $2\omega + 1$. We have $\theta_{t,0} = 1$, $\theta_{t,1} = M(t) - 1$, $\theta_{t,2\omega} = 1$, $\psi_{t,0} = 1$, $\psi_{t,1} = M(t) + 1$, $\psi_{t,2\omega} = -1$.

From the relation $\theta_{t,2\omega+1} = M(t)\theta_{t,2\omega} - \theta_{t,2\omega-1}$, we obtain $\theta_{t,2\omega-1} = M(t) - 1$. It is seen that $\theta_{t,2\omega-1} = \theta_{t,1}$ and $\theta_{t,2\omega-1} = -\psi_{t,1}$. As a consequence of Corollary 5.2, it follows that the subsets $\{\theta_{t,0}, \theta_{t,1},\ \dots, \theta_{t,\omega-1}\}$ and $\{\theta_{t,\omega+1}, \theta_{t,\omega+2},\ \dots,\ \theta_{t,2\omega+1}\}$ have symmetric property about the middlemost element $\theta_{t,\omega}$ while the subsets $\{\psi_{t,0}, \psi_{t,1},\ \dots,\ \psi_{t,\omega-1}\}$ and $\{\psi_{t,\omega+1}, \psi_{t,\omega+2},\ \dots,$ $\psi_{t,2\omega+1}\}$ possess skew-symmetric property about the middlemost element $\psi_{t,\omega}$.

Theorem 5.5 (Effect of the transformations)**.** *The symmetric and skew-symmetric properties of* $\{\theta_{t,k} \pmod{\rho}\}$ *and* $\{\psi_{t,k} \pmod{\rho}\}$*-sequences are preserved under the transformations* τ_t *and* σ_t*, respectively.*

Proof. Assume $h \geq j+2$. Suppose the subsets $\{\theta_{t,j}, \theta_{t,j+1}\}$ and $\{\theta_{t,h-1}, \theta_{t,h}\}$ in $\mathfrak{C}_1(t)$ have symmetric property. Then we have $\theta_{t,j} = \theta_{t,h}$ and $\theta_{t,j+1} = \theta_{t,h-1}$. Consequently $\tau_t\,(\theta_{t,j}) = \tau_t\,(\theta_{t,h})$ and $\tau_t\,(\theta_{t,j+1}) = \tau_t\,(\theta_{t,h-1})$. By Theorem 4.2, we obtain $\theta_{t+1,j} = \theta_{t+1,h}$ and $\theta_{t+1,j+1} = \theta_{t+1,h-1}$. i.e., the subsets $\{\theta_{t+1,j}, \theta_{t+1,j+1}\}$ and $\{\theta_{t+1,h-1}, \theta_{t+1,h}\}$ in $\mathfrak{C}_1(t+1)$ have symmetric property.

Next suppose that $s \geq r+2$ and the subsets $\{\psi_{t,r}, \psi_{t,r+1}\}$ and $\{\psi_{t,s-1}, \psi_{t,s}\}$ in $\mathfrak{C}_1(t)$ have skew-symmetric property. Then $\psi_{t,r} = -\psi_{t,s}$ and $\psi_{t,r+1} = -\psi_{t,s-1}$. Since the corresponding elements in the $\theta_{t,k} \pmod{\rho}$-sequence possess symmetric property, we get $\theta_{t,r} = \theta_{t,s}$ and $\theta_{t,r+1} = \theta_{t,s-1}$.

Application of Theorem 4.5 yields $\psi_{t+1,r} = \sigma_t(\theta_{t,r}, \psi_{t,r}) = \sigma_t(\theta_{t,s}, -\psi_{t,s}) = -\sigma_t(\theta_{t,s}, \psi_{t,s}) = -\psi_{t+1,s}$ and $\psi_{t+1,r+1} = \sigma_t(\theta_{t,r+1}, \psi_{t,r+1}) = \sigma_t(\theta_{t,s-1}, -\psi_{t,s-1}) = -\sigma_t(\theta_{t,s-1}, \psi_{t,s-1}) = -\psi_{t+1,s-1}$. Therefore, the subsets $\{\psi_{t+1,r}, \psi_{t+1,r+1}\}$ and $\{\psi_{t+1,s-1}, \psi_{t+1,s}\}$ in $\mathfrak{C}_1(t+1)$ possess skew-symmetric property. By Corollary 5.2, the symmetric and skew-symmetric sets with two elements each can be extended further. This completes the proof. □

5.6 Determination of the middlemost elements in the rows of $\mathfrak{C}_1(t)$

Now we take up an important requirement in our study, namely the determination of the middlemost elements in the compartments. Around the middlemost elements in the rows of $\mathfrak{C}_1(t)$, we have

$$\theta_{t,\omega-1} = \theta_{t,\omega+1} \tag{5.16}$$

and

$$\psi_{t,\omega-1} = -\psi_{t,\omega+1}. \tag{5.17}$$

By Theorem 2.1, we have

$$\psi_{t,\omega+1} - \theta_{t,\omega+1} = \theta_{t,\omega} + \psi_{t,\omega}. \tag{5.18}$$

Using (5.16) and (5.17), we obtain

$$\psi_{t,\omega-1} + \theta_{t,\omega-1} = -(\theta_{t,\omega} + \psi_{t,\omega}). \tag{5.19}$$

Again by Theorem 2.1, we have

$$\psi_{t,\omega} - \theta_{t,\omega} = \theta_{t,\omega-1} + \psi_{t,\omega-1}. \tag{5.20}$$

Using (5.19), we obtain

$$\psi_{t,\omega} - \theta_{t,\omega} = -(\theta_{t,\omega} + \psi_{t,\omega}).$$

This gives the result

$$\psi_{t,\omega} = 0 \tag{5.21}$$

which plays a crucial role in the further development of our method of cyclic sequences. Applying Theorem 2.2 we obtain $\theta_{t,\omega}\psi_{t,\omega+1} = 2$. This implies $\psi_{t,\omega+1} \neq 0$ and hence we have

$$\theta_{t,\omega} = \frac{2}{\psi_{t,\omega+1}} \tag{5.22}$$

where $\dfrac{1}{\psi_{t,\omega+1}}$ is the multiplicative inverse of $\psi_{t,\omega+1}$ in $\mathbb{F}_\rho$.

From (2.3), we obtain $\theta_{t,\omega+1} = M(t)\theta_{t,\omega} - \theta_{t,\omega-1}$.

Using (5.16), we get $\theta_{t,\omega+1} = M(t)\theta_{t,\omega} - \theta_{t,\omega+1.}$ So we have 2 $\theta_{t,\omega+1} = M(t)\theta_{t,\omega}$.

Because of (5.22) we have

$$\theta_{t,\omega+1} = \frac{M(t)}{\psi_{t,\omega+1}}. \tag{5.23}$$

The relations (5.18) and (5.21) give $\psi_{t,\omega+1} = \theta_{t,\omega} + \theta_{t,\omega+1}$. Using (5.22) and (5.23), we obtain $\psi_{t,\omega+1} = \frac{2}{\psi_{t,\omega+1}} + \frac{M(t)}{\psi_{t,\omega+1}}$. Therefore, $\psi^2_{t,\omega+1} = \{M(t-1)\}^2$. This gives $\psi_{t,\omega+1} = \pm M(t-1)$. In view of this result, the relations (5.22) and (5.23) yield $\theta_{t,\omega} = \pm\frac{2}{M(t-1)}$ and $\theta_{t,\omega+1} = \pm\frac{M(t)}{M(t-1).}$ We assert that the - sign cannot hold in the expression for $\theta_{t,\omega}$. If $\theta_{t,k} = -\frac{2}{M(t-1)}$ then from Theorem 4.2 we have $\theta_{t+1,\omega} = \tau_t(\theta_{t,\omega}) = \frac{2}{M(t)}, \cdots, \theta_{t+n,\omega} = \frac{2}{M(t-1)} \neq \theta_{t,\omega}$ which is a contradiction. Thus our assertion holds. Hence we have

$$\theta_{t,\omega} = \frac{2}{M(t-1)}. \tag{5.24}$$

It follows that $\theta_{t,\omega+1} = \frac{M(t)}{M(t-1)}$ and $\psi_{t,\omega+1} = M(t-1)$. Thus we obtain the following elements in the $\theta_{t,k} \pmod{\rho}$ and $\psi_{t,k} \pmod{\rho}$-sequences, corresponding to $k = \omega - 1, \omega$ and $\omega + 1$ as shown in Table 5.1.

Table 5.1. Values at $\omega - 1$, ω and $\omega + 1$

k	$\cdots$	$\omega - 1$	ω	$\omega + 1$
$\theta_{t,k}$	$\cdots$	$\frac{M(t)}{M(t-1)}$	$\frac{2}{M(t-1)}$	$\frac{M(t)}{M(t-1)}$
$\psi_{t,k}$	$\cdots$	$-M(t-1)$	0	$M(t-1)$

5.7 Uniqueness of the middlemost entries in the rows of $\mathfrak{C}_1(t)$

One can establish that there does not exist a positive integer $j \neq \omega$ such that

$$\theta_{t,j} = \frac{2}{M(t-1)} \tag{5.25}$$

in $\mathfrak{C}_1(t)$. The proof is by contradiction, employing Theorem 2.2 and the method described earlier for the determination of the neighboring elements. Thus we obtain the following result.

Theorem 5.6. *The middlemost positions in each compartment of $\mathfrak{a}(M(t))$ are occupied by the values of $\frac{2}{M(t-1)}$ and 0 in the first and second rows, respectively and these values are not attained at any other places in the concerned compartment.*

The following distinguishing characteristic emerges:

Remark 5.1. *It is seen that Theorems 4.3 and 5.6 bring out the distinguishing feature of $\theta_{t,k} \pmod{\rho}$ and $\psi_{t,k} \pmod{\rho}$-sequences, namely that the $\theta_{t,k}$-sequence never attains the value of 0 whereas the $\psi_{t,k}$-sequence attains zero exactly once in each compartment of $\mathfrak{a}(M(t))$.*

Remark 5.2. *Given M(t), it follows from equation* (5.21) *that ω is the smallest positive integer such that $\psi_{t,\omega}$ attains the value of zero in $\mathbb{F}_\rho$.*

Definition 5.4 (Pivotal elements in $\mathfrak{C}_1(t)$)**.** *The pair of middlemost entries in the first and second rows of $\mathfrak{C}_1(t)$ are referred to as the pivotal elements of $\mathfrak{C}_1(t)$. The middlemost position in the first or the second row of $\mathfrak{C}_1(t)$ is called the pivotal position of $\mathfrak{C}_1(t)$.*

Theorem 5.7. *For the M-cycle given by* (4.1)*, all the $\mathfrak{C}_1(t)$-compartments in the matrix $\mathfrak{a}(t)$ have the same pair of pivotal elements, for all the positive integral values of t.*

Proof. For a given $t \in N$, let the pivotal position of $\mathfrak{C}_1(t)$ in $\mathfrak{a}(t)$ be ω. Then $\theta_{t,\omega} = \frac{2}{M(t-1)}$ and $\psi_{t,\omega} = 0$. By Theorem 4.5, we have $\psi_{t+1,\omega} = \sigma_t\ (\theta_{t,\omega},\ \psi_{t,\omega}) = 0$. Since the ψ-sequence assumes the value of 0 only once in a compartment, it follows that the pivotal position of the compartment $\mathfrak{C}_1(t+1)$ in $\mathfrak{a}(t+1)$ is also ω. Hence the theorem follows. □

Corollary 5.3 (Transformation of the pivotal elements)**.** *The pivotal elements in $\mathfrak{C}_1(t)$ are transformed by τ_t and σ_t into the respective pivotal elements in $\mathfrak{C}_1(t+1)$.*

Proof. We have

$$\tau_t(\theta_{t,\omega}) = \tau_t(\frac{2}{M(t-1)}) = \frac{2}{M(t)} = \theta_{t+1,\omega} \tag{5.26}$$

and

$$\sigma_t(\theta_{t,\omega}, \psi_{t,\omega}) = \theta_{t,\omega}\psi_{t,\omega} = 0 = \psi_{t+1,\omega} \tag{5.27}$$

The theorem follows from (5.26) and (5.27). □

Corollary 5.4 (Periodicity of the $\{\theta_{t,k}\}$ and $\{\psi_{t,k}\}$-sequences)**.** *Consider the cycle $M(t) = M_1 \to M_2 \to \cdots \to M_n \to M_{n+1} = M_1$ in $\mathbb{F}_\rho$ as per* (4.1)*. For each t, the period of the cyclic sequence $\theta_{t,k}$ (respectively, $\psi_{t,k}$) as a function of k is $2\omega + 1$.*

6 Existence of roots of polynomials of $H(x)$-sequence in finite fields

The existence of a nontrivial M-cycle has been established in Theorem 3.4. Given $M(t)$, we have seen in Section 5, how the $\theta_{t,k} \pmod{\rho}$ and $\psi_{t,k} \pmod{\rho}$-sequences, considered as functions of t, split into several identical parts. A remarkable property in the determination of the structure of such parts is provided by equation (5.21), viz. the existence of a least positive integer ω such that $\psi_{t,\omega} = 0$. This implies that M(t) satisfies the polynomial $H_\omega(x)$. If ω = 1, then $\psi_{t,1}$ = 0 implies $M(t) = -1$ from which we get the M-cycle $-1 \to -1 \to -1 \to \ldots$ Thus M(t) contributes the root of the polynomial $H_1(x)$. Consider the case when $\omega > 1$ so that we have $n > 1$. Take the cycle $M(t) = M_1 \to M_2 \to \cdots \to M_n \to M_{n+1} = M_1$ in $\mathbb{F}_\rho$ given by (4.1). By Corollary 5.3, it follows that $\psi_{t+1,\omega} = 0, \ldots, \psi_{t+n,\omega} = 0$. Therefore the elements $M(t), M(t+1), \ldots, M(t+n-1)$ satisfy the polynomial $H_\omega(x)$ over $\mathbb{F}_\rho$. Hence $(x - M(t))(x - M(t+1)) \cdots (x - M(t+n-1)) \mid H_\omega(x)$. So the $M(t)$-cycle in $\mathbb{F}_\rho$ contributes n roots of the polynomial $H_\omega(x)$. Thus the existence of a nontrivial M-cycle of length n in $\mathbb{F}_\rho$ implies the existence of n roots of the $H(x)$-polynomial in $\mathbb{F}_\rho$. Since the degree of $H_\omega(x)$ is ω, we have

$$\omega \geq n. \tag{6.1}$$

Conversely, suppose α is a root of $H_\omega(x)$ in $\mathbb{F}_\rho$. Choose d as the least positive integer such that $2d + 1 \mid 2\omega + 1$ and α is a root of $H_d(x)$. Since the constant term of any polynomial in the $H(x)$-sequence is either 1 or -1, it follows that $\alpha \neq 0$. Since the sum of the coefficients of any

polynomial in the $H(x)$-sequence is one of $\pm 1, \pm 2$, we have $\alpha \neq 1$. By induction, we obtain the following results:

$$H_k(2) = 2k + 1, \ \forall\, k \geq 0,$$

$$H_k(-2) = \begin{cases} 1, & \text{if } k \text{ is even,} \\ -1, & \text{if } k \text{ is odd.} \end{cases}$$

So $\alpha \neq \pm 2$. If $\alpha^2 = 2$, then $H_k(\alpha) = \pm 1, \pm(\alpha + 1), \forall\ k \geq 0$. Hence $H_d(x)$ = 0 implies $\alpha = -1$. In this case, we get the sequence $-1 \to -1 \to -1 \to \cdots$ This implies $\omega = 1$. If $\alpha^2 = 3$, then $H_k(\alpha) = \pm 1,\ \pm(\alpha + 1), \pm(\alpha + 2),\ \forall\, k \geq 0$. Hence $H_d(x) = 0$ implies that $\alpha = -2$ or -1. Since α cannot be -2, we have $\alpha = -1$, which has already been accounted for. Consider the case when $\alpha \neq -1$. Then $\alpha^2 \neq 2,\ 3$ and so $\omega \neq 1$. Define $M_k = F_k(\alpha) \pmod{\rho}$ $(k \geq 1)$, where F is defined by the relation (2.1). We obtain the sequence $\alpha \to \alpha^2 - 2 \to \alpha^4 - 4\alpha^2 + 2 \to \cdots$ Since the conditions of Theorem 3.1 are satisfied, the above sequence is non-stationary. Thus we obtain an $M(t)$-cycle of length n. The foregoing discussion shows that $\psi_{t+1,d} = 0, \ldots, \psi_{t+n,d} = 0$. Hence a root α of the polynomial $H_d(x)$ in $\mathbb{F}_\rho$ gives rise to an $M(t)$-cycle of length n such that each element of this cycle is a root of the polynomial $H_d(x)$. Thus we are led to an important result on the attainment of the roots of the $H(x)$-polynomial stated as follows:

Theorem 6.1 (Necessary and sufficient condition)**.** *Let ρ be a given odd prime $\geq$ 11. An $M(t)$-cycle of length n exists in the field $\mathbb{F}_\rho$ if and only if there exists a positive integer $\omega \geq n$ such that the polynomial $H_\omega(x)$ attains roots at n distinct elements of $\mathbb{F}_\rho$ with pivotal position ω in the compartments $\mathfrak{C}_1(t)$, $\mathfrak{C}_1(t+1)$, …, $\mathfrak{C}_1(t+n-1)$ of the matrices $\mathfrak{a}(M(t))$, $\mathfrak{a}(M(t+1))$, …, $\mathfrak{a}(M(t+n-1))$, respectively. One can choose ω as the least positive integer with this property.*

Corollary 6.1. *If α is a root of $H_\omega(x)$ in $\mathbb{F}_\rho$, then $\alpha^2 - 2$ is also a root of $H_\omega(x)$.*

Corollary 6.2. *Every root of an $H(x)$-polynomial occurring in $\mathbb{F}_\rho$ is an element of a unique M-cycle.*

7 A relationship involving the pivotal position in $\mathfrak{C}_1(t)$

The concept of pivotal elements in a compartment was introduced in Section 5. Now we consider the identification of a relationship involving the pivotal position of the compartment $\mathfrak{C}_1(t)$.

7.1 Formation of new sequences

Let the parameter t be given. We form two new sequences as follows: η-sequence is formed with the sums of two consecutive terms of the ψ-sequence; ζ-sequence is formed from ψ-sequence by taking the terms from $\psi_{t,\omega}$ onwards. We have the following definition.

Definition 7.1. *Let ω be the pivotal position in the compartment $\mathfrak{C}_1(t)$. Define*

$$\eta_{t,k} = \psi_{t,k-1} + \psi_{t,k}, \tag{7.1}$$

$$\zeta_{t,k} = \psi_{t,\omega+k}. \tag{7.2}$$

By induction, we obtain a remarkable relationship between the two sequences.

Theorem 7.1. *The following property holds:*

$$\eta_{t,k} = M(t-1)\zeta_{t,k}, \forall\ k \geq 1. \tag{7.3}$$

Corollary 7.1. *It holds that*

$$\psi_{t,k-1} + \psi_{t,k} = M(t-1)\psi_{t,\omega+k},\ \forall\ k \geq 1. \tag{7.4}$$

Using the relation $\psi_{t,2\omega+1+k} = \psi_{t,k}$, we obtain a result.

Corollary 7.2. *The following relationship holds:*

$$\psi_{t,\omega+k} + \psi_{t,\omega+k+1} = M(t-1)\psi_{t,k},\ \forall\ k \geq 0. \tag{7.5}$$

7.2 Preliminaries for building blocks

By induction, we obtain some important relationships.

Theorem 7.2. *The following properties hold:*

$$\psi_{t,2k} + \psi_{t,2k+1} = \{M(t)+2\}\psi_{t+1,k},\ \forall\ k \geq 0. \tag{7.6}$$

$$\theta_{t,k}\psi_{t,k+1} + \theta_{t,k+1}\psi_{t,k} = 2\ \psi_{t+1,\omega+k+1},\ \forall\ k \geq 0. \tag{7.7}$$

Theorem 7.3. *The following relationship holds:*

$$(\theta_{t,k} + \theta_{t,k+1})(\psi_{t,k} + \psi_{t,k+1}) = \{M(t)+2\}\psi_{t+1,\omega+k+1},\ \forall\ \ k \geq 0. \tag{7.8}$$

Proof. Applying Theorem 4.4 and the relation (7.7), we obtain $(\theta_{t,k} + \theta_{t,k+1})(\psi_{t,k} + \psi_{t,k+1}) = \psi_{t+1.k} + \psi_{t+1,k+1} + 2\psi_{t+1,\omega+k+1}$. In view of Corollary 7.1, the latter expression reduces to $\{M(t)+2\}\psi_{t+1,\omega+k+1}$. □

We deduce a relationship between the pivotal position in $\mathfrak{C}_1(t)$ and an element of the M-cycle.

Corollary 7.3. *The following holds:*

$$\psi_{t,k}^2 - \ \psi_{t,k-1}^2 = \{M(t)+2\}\psi_{t+1,\omega+k},\ \forall\ k \geq 1. \tag{7.9}$$

Proof. Follows from Theorem 2.1. □

The next theorem provides us with a mechanism to link the $\{\psi_{t,k}\}$-sequence with the Mersenne, Fermat and Lehmer numbers. By repeated application of the relation (7.6), we obtain

Theorem 7.4. *Suppose $q = 2^i$ for some positive integer i. Then*

$$\sum_{j=0}^{q-1} \psi_{t,j} = \{M(t)+2\}\{M(t+1)+2\}\cdots\{M(t+i-1)+2\}. \tag{7.10}$$

7.3 Blocks of ψ-sequences

Blocks are formed from ψ-sequence by taking consecutive terms such that the cardinality of each block is an integral power of 2.

Definition 7.2 (ψ-Block at t)**.** *We define a block of numbers from ψ-sequence as follows:* $\mathfrak{B}_0(t) = \{\psi_{t,1}\}$ *and* $\mathfrak{B}_k(t) = \{\psi_{t,2^k}, \psi_{t,2^k+1}, \cdots, \psi_{t,2^{k+1}-1}\}$, $\forall\ k \geq 1$. *We have* $\#\mathfrak{B}_k(t) = 2^k$.

Definition 7.3 (Block sum)**.** *Let $S(\mathfrak{B}_k(t))$ denote the sum of the numbers in $\mathfrak{B}_k(t)$. i.e.,*

$$S(\mathfrak{B}_k(t)) = \sum_{j=q}^{r-1} \psi_{t,j} \text{ where } q = 2^k \text{ and } r = 2^{k+1}. \tag{7.11}$$

Theorem 7.5. *It holds that*

$$S(\mathfrak{B}_1(t)) = \{M(t) + 2\} S(\mathfrak{B}_0(t+1)). \tag{7.12}$$

Proof. Using the relation (7.6) we obtain

$$\begin{aligned} S(\mathfrak{B}_1(t)) &= \psi_{t,2} + \psi_{t,3} \\ &= \{M(t) + 2\}\psi_{t+1,1} \\ &= \{M(t) + 2\} S(\mathfrak{B}_0(t+1)). \end{aligned}$$

□

Theorem 7.6 (Formula for S($\mathfrak{B}_k$(t)))**.** *The following holds:*

$$S(\mathfrak{B}_k(t)) = \{M(t+k) + 1\} \prod_{j=1}^{k} \{M(t+j-1) + 2\}. \tag{7.13}$$

Proof. We have S($\mathfrak{B}_2$(t)) = $\sum_{j=4}^{7} \psi_{t,j}$. Using Theorem 7.2, we get

$$\begin{aligned} S(\mathfrak{B}_2(t)) &= \{M(t) + 2\}(\psi_{t+1,2} + \psi_{t+1,3}) \\ &= \{M(t) + 2\} S(\mathfrak{B}_1(t+1)) \\ &= \{M(t) + 2\}\{M(t+1) + 2\} S(\mathfrak{B}_0(t+2)), \end{aligned}$$

by Theorem 7.5. Continuing this process, we obtain (7.13). □

7.4 Product of two consecutive terms in the ψ-sequence

Our requirement now is to find an expression for $\psi_{t,k-1}\psi_{t,k}$.

Theorem 7.7. *The following relation holds:*

$$\psi_{t,2^k-1}\psi_{t,2^k} - \psi_{t,2^{k-1}-1}\psi_{t,2^{k-1}} = \{M(t)+2\}\{\psi_{t+1,2^k-1} + \psi_{t+1,2^k-2} + \cdots + \psi_{t+1,2^{k-1}+1} + \psi_{t+1,2^{k-1}}\} \tag{7.14}$$

Proof. From (2.4), we have $\psi_{t,k} = M(t)\psi_{t,k-1} - \psi_{t,k-2}$. This gives $\psi_{t,k-2} + \psi_{t,k} = M(t)\psi_{t,k-1}$. Multiplying both sides by $\psi_{t,k-1}$, we obtain $\psi_{t,k-2}\psi_{t,k-1} + \psi_{t,k-1}\psi_{t,k} = M(t)\psi_{t,k-1}^2$. Similarly we obtain $\psi_{t,k-3}\psi_{t,k-2} + \psi_{t,k-2}\psi_{t,k-1} = M(t)\psi_{t,k-2}^2$, etc.

From these relations, we get

$$\psi_{t,k-1}\psi_{t,k} + \psi_{t,0}\psi_{t,1} = M(t)(\psi_{t,k-1}^2 - \psi_{t,k-2}^2 + \psi_{t,k-3}^2 - \cdots + \psi_{t,3}^2 - \psi_{t,2}^2 + \psi_{t,1}^2)$$

and

$$\psi_{t,k-1}\psi_{t,k} - \psi_{t,0}\psi_{t,1} = M(t)(\psi^2_{t,k-1} - \psi^2_{t,k-2} + \psi^2_{t,k-3} - \cdots - \psi^2_{t,3} + \psi^2_{t,2} - \psi^2_{t,1}),$$

for n even and odd, respectively.

Using Corollary 7.3, we obtain the relations

$$\begin{aligned}\psi_{t,k-1}\psi_{t,k} &= M(t)\{M(t)+2\}(\psi_{t+1,\omega+k-1} + \psi_{t+1,\omega+k-3} + \cdots + \psi_{t+1,\omega+3}) + \\ &\quad \{M(t)+1\}\{(M(t))^2 - M(t) - 1\} \text{ for } k \text{ even,} \end{aligned} \tag{7.15}$$

$$\begin{aligned}\psi_{t,k-1}\psi_{t,k} &= M(t)\{M(t)+2\}(\psi_{t+1,\omega+k-1} + \psi_{t+1,\omega+k-3} + \cdots + \psi_{t+1,\omega+2}) + \\ &\quad \{M(t)+1\}\{(M(t))^2 - M(t) - 1\} \text{ for } k \text{ odd.} \end{aligned} \tag{7.16}$$

Replacing k in (7.15) by 2^k and in (7.16) by 2^{k-1}, respectively, we get the relations

$$\begin{aligned}\psi_{t,2^k-1}\psi_{t,2^k} &= M(t)\{M(t)+2\}(\psi_{t+1,\omega+2^k-1} + \psi_{t+1,\omega+2^k-3} + \cdots \\ &\quad +\psi_{t+1,\omega+3}) + \{M(t)+1\}\{(M(t))^2 - M(t) - 1\}, \end{aligned} \tag{7.17}$$

$$\begin{aligned}\psi_{t,2^{k-1}-1}\psi_{t,2^{k-1}} &= M(t)\{M(t)+2\}(\psi_{t+1,\omega+2^{k-1}-1} + \psi_{t+1,\omega+2^{k-1}-3} + \cdots \\ &\quad +\psi_{t+1,\omega+3}) + \{M(t)+1\}\{(M(t))^2 - M(t) - 1\}. \end{aligned} \tag{7.18}$$

From the relations (7.17) and (7.18), we get $\psi_{t,2^k-1}\psi_{t,2^k} - \psi_{t,2^{k-1}-1}\psi_{t,2^{k-1}}$
$= \{M(t)+2\}(\psi_{t+1,\omega+2^k-1} + \psi_{t+1,\omega+2^k-3} + \cdots + \psi_{t+1,\omega+2^{k-1}+1})$
$= \{M(t)+2\}(\psi_{t+1,2^k-1} + \psi_{t+1,2^k-2} + \cdots + \psi_{t+1,2^{k-1}+1} + \psi_{t+1,2^{k-1}})$, using Corollary 7.2. □

Theorem 7.8. *Let $q = 2^i$, $r = 2^{i+1}$ and $s = 2^{i-1}$. Then*

$$\sum_{j=q}^{r-1} \psi_{t,j} = \psi_{t,q-1}\,\psi_{t,q} - \psi_{t,s-1}\psi_{t,s}. \tag{7.19}$$

Proof. From the relation (7.14), we have $\psi_{t,q-1}\,\psi_{t,q} - \psi_{t,s-1}\psi_{t,s} = \{M(t)+2\}S(\mathfrak{B}_{i-1}(t+1)) = S(\mathfrak{B}_i(t))$, yielding (7.19). □

Theorem 7.9. *The following property holds:*

$$\{M(t)-2\}(\psi_{t,2^k-1}\psi_{t,2^k} - \psi_{t,2^{k-1}-1}\psi_{t,2^{k-1}}) = M(t+k+1) - M(t+k). \tag{7.20}$$

Proof. From Theorem 7.8, we have

$$\psi_{t,2^k-1}\psi_{t,2^k} - \psi_{t,2^{k-1}-1}\psi_{t,2^{k-1}} = S(\mathfrak{B}_k(t)) = \{M(t+k)+1\}\prod_{j=1}^{k}\{M(t+j-1)+2\}.$$

Hence we obtain

$$\begin{aligned}&\{M(t)-2\}(\psi_{t,2^k-1}\psi_{t,2^k} - \psi_{t,2^{k-1}-1}\psi_{t,2^{k-1}}) \\ &= \{M(t)-2\} \times \{M(t+k)+1\}\prod_{j=1}^{k}\{M(t+j-1)+2\},\end{aligned} \tag{7.21}$$

in view of the relation (7.13). We expand the right side of (7.21) and carry out the computations successively. First we have $\{M(t)-2\}\{M(t)+2\} = \{M(t)\}^2 - 4 = M(t+1) - 2$.

Next we have $\{M(t)-2\}\{M(t)+2\}\{M(t+1)+2\} = \{M(t+1)-2\}\{M(t+1)+2\} = \{M(t)\}^2 - 4 = M(t+2)-2$, and so on. Therefore the right side of (7.21) reduces to $\{M(t+k)+1\}\{M(t+k)-2\} = \{M(t+k)\}^2 - M(t+k) - 2 = M(t+k+1) - M(t+k)$. □

Theorem 7.10. *The following identity holds:*

$$\{M(t)-2\}\psi_{t,2^k-1}\psi_{t,2^k} = M(t+k+1) - M(t). \tag{7.22}$$

Proof. Using the property provided by the relation (7.20), we successively get

$$\left.\begin{array}{c} \{M(t)-2\}(\psi_{t,2^k-1}\psi_{t,2^k} - \psi_{t,2^{k-1}-1}\psi_{t,2^{k-1}}) = M(t+k+1) - M(t+k), \\ \{M(t)-2\}(\psi_{t,2^{k-1}-1}\psi_{t,2^{k-1}} - \psi_{t,2^{k-2}-1}\psi_{t,2^{k-1}-1}) = M(t+k) - M(t+k-1), \\ \vdots \\ \{M(t)-2\}(\psi_{t,3}\psi_{t,4} - \psi_{t,1}\psi_{t,2}) = M(t+3) - M(t+2), \\ \{M(t)-2\}(\psi_{t,1}\psi_{t,2} - \psi_{t,0}\psi_{t,1}) = M(t+2) - M(t+1). \end{array}\right\}$$

Adding vertically the above relations, we obtain $\{M(t)-2\}(\psi_{t,2^k-1}\psi_{t,2^k} - \psi_{t,0}\psi_{t,1}) = M(t+k+1) - M(t+1)$. This gives

$$\begin{aligned} \{M(t)-2\}\psi_{t,2^k-1}\psi_{t,2^k} &= M(t+k+1) - M(t+1) + \{M(t)-2\}\{M(t)+1\} \\ &= M(t+k+1) - M(t). \end{aligned}$$ □

8 Divisors of Mersenne and Lehmer numbers

We exhibit a relationship that the cyclic sequences $\{\theta_{t,k} \pmod{\rho}\}$ and $\{\psi_{t,k} \pmod{\rho}\}$ have with Mersenne and Lehmer numbers. Let t be varying. For each fixed k, it has been proved in Section 4 that the cyclic sequences are periodic with the same period as that of the cycle $M_1 \to M_2 \to \cdots \to M_n \to M_{n+1} = M_1$. From this result, we obtain the following:

Theorem 8.1. *Let n be a positive integer. The following statements are equivalent:*

(a) $\theta_{t+n,1} = \theta_{t,1}$,

(b) $\psi_{t+n,1} = \psi_{t,1}$,

(c) $M(t+n) = M(t)$.

Putting the different pieces from the previous sections in a comprehensive way, we obtain the following result fulfilling the objective of this study.

Theorem 8.2 (Divisors of Mersenne and Lehmer numbers)**.** *Let ρ be an odd prime ≥ 11. Let $M(t) \in \mathbb{F}_\rho - \{0, \pm 1, \pm 2\}$ such that $M_k^2 \neq 2, 3,\ \forall\ k$ in the cycle $M(t) = M_1 \to M_2 \to \cdots \to M_n \to M_{n+1} = M_1 \to \cdots$, where $M_k = M(t+k-1) = M_{k-1}^2 - 2$. Define $\psi_{t,0} = 1$, $\psi_{t,1} = M(t) + 1$, $\psi_{t,k} = M(t)\psi_{t,k-1} - \psi_{t,k-2}, \forall\ k \geq 2$. Let ω be the smallest number in N such that $\psi_{t,\omega} = 0$. Then $2\omega + 1$ divides either the Mersenne number $2^n - 1$ or the Lehmer number $2^n + 1$.*

Proof. Since the M-cycle has length n, we get $M(t+n) = M(t)$. This gives $M(t+n)-M(t) = 0$. From Theorem 6.1, it follows that there exists a smallest natural number ω such that $\psi_{t,\omega} = 0$ for all t defining the M-cycle. For each t, by Corollary 5.4, the period of the cyclic sequence $\psi_{t,k}$ as a function of k is $2\omega+1$. Hence we have $\psi_{t,k} = 0$ for all natural numbers k of the form $j(2\omega+1)+\omega$, where j is a non-negative integer. In view of the identity provided by Theorem 7.10, we obtain $\{M(t) - 2\}\psi_{t,2^{n-1}-1}\psi_{t,2^{n-1}} = 0$ for all t defining the M-cycle. Since $M(t) \neq 2$, we have either $\psi_{t,2^{n-1}-1} = 0$ or $\psi_{t,2^{n-1}} = 0$. Hence the $\psi_{t,k}$-sequence attains a root when $k = 2^{n-1} - 1$ or 2^{n-1}. This implies that either $2^{n-1} - 1$ or 2^{n-1} is of the form $j(2\omega + 1) + \omega$ for some integer $j \geq 0$.
Case (i). Suppose

$$2^{n-1} - 1 = j(2\omega + 1) + \omega. \tag{8.1}$$

Then $2\{j(2\omega + 1) + \omega\} + 1 = 2^n - 1$, i.e., $(2j + 1)(2\omega + 1) = 2^n - 1$, implying $2\omega + 1 \mid 2^n - 1$.
Case (ii). Suppose

$$2^{n-1} = j(2\omega + 1) + \omega. \tag{8.2}$$

Then $2\{j(2\omega+1)+\omega\}+1 = 2^n+1$, i.e., $(2j+1)(2\omega+1) = 2^n+1$. Hence $2\omega+1 \mid 2^n+1$. □

Thus the ψ-sequence leads to a factor $2\omega + 1$ of the Mersenne number $2^n - 1$ in Case (i) and the Lehmer number $2^n + 1$ in Case (ii).

Theorem 8.3 (Relationship concerning n, ω and Euler's function)**.** *Given an $M(t)$-cycle of length n in $\mathbb{F}_\rho$ with the occurrence of the roots of the corresponding polynomial $H(x)$ in the $\psi_{t,k}$-sequence at $k = \omega$, we have*

$$n \mid \frac{1}{2}\Phi(2\omega + 1), \tag{8.3}$$

where Φ is Euler's totient function.

Proof. From Theorem 8.2 we have $2\omega + 1 \mid 2^{2n} - 1$. By Euler's generalization of Fermat's theorem, $2\omega + 1 \mid 2^{\Phi(2\omega+1)} - 1$. These two relations imply that $2n \mid \Phi(2\omega + 1)$. □

The theory presented by means of Theorems 6.1, 8.2 and 8.3 is illustrated below.

Example 8.1. *Consider the field $\mathbb{F}_\rho$ with $\rho = 137$. We have $(\frac{28}{137}) = 1$. On computation, $113^2 = 12769 \equiv 28 \pmod{137}$. Hence $113^2 - 2 \equiv 26 \pmod{137}$. Starting with $M(t) = 26$, we get the cycle $26 \to 126 \to 119 \to 48 \to 110 \to 42 \to 118 \to 85 \to 99 \to 72 \to 113 \to 26 \to \cdots$ in $\mathbb{F}_\rho$ of length 11. The $\Psi-$sequence corresponding to $M(t) = 26$ is $\Psi_{t,0} = 1$, $\Psi_{t,1} = 27$, $\Psi_{t,2} = 16, \ldots$, which attains the value of zero at $\omega = 11$. In view of Theorem 6.1, the M-cycle provides 11 roots of $H_{11}(x)$ in $\mathbb{F}_\rho$. By Theorem 8.2, we get $23 \mid 2^{11} \pm 1$. We note that $23 \mid 2^{11} - 1$.*

Example 8.2. *Consider the field $\mathbb{F}_\rho$ with $\rho = 1283$. We find that $(\frac{13}{1283}) = 1$. So $1247^2 = 1555009 \equiv 13 \pmod{1283}$ and $1247^2 - 2 \equiv 11 \pmod{1283}$. Taking $M(t) = 11$, we obtain the M-cycle $11 \to 119 \to 46 \to 831 \to 305 \to 647 \to 349 \to 1197 \to 979 \to 38 \to 159 \to 902 \to 180 \to 323 \to 404 \to 273 \to 113 \to 1220 \to 118 \to 1092 \to 555 \to 103 \to 343 \to 894 \to 1208 \to 491 \to 1158 \to 227 \to 207 \to 508 \to 179 \to 1247 \to 11 \to \cdots$ in $\mathbb{F}_\rho$ of length 32. The $\Psi-$sequence corresponding to $M(t) = 11$ is $\Psi_{t,0} = 1$, $\Psi_{t,1} = 12$, $\Psi_{t,2} = 131, \ldots$, which attains the value of zero at $\omega = 320$. In view of Theorem 6.1, the M-cycle contributes 32 roots of $H_{320}(x)$ in $\mathbb{F}_\rho$. Using Theorem 8.2 we see that $641 \mid 2^{32} \pm 1$. It is checked that $641 \mid 2^{32} + 1$. Thus we have a proof for Euler's result on a prime factor of the fifth Fermat number.*

9 Conclusion

In the material that has been hitherto presented, we have established how an M-cycle in the finite field $\mathbb{F}_\rho$ yields the factors of Mersenne, Fermat and Lehmer numbers. It is pertinent to consider the converse result. A question that arises is how to find the $M-$cycles from the factors of given Mersenne, Fermat and Lehmer numbers. This will be taken up in a subsequent study.

Acknowledgements

The author sincerely thanks the reviewers for the suggestions towards the betterment of the paper.

References

[1] Brillhart, J. (1964). On the factors of certain Mersenne numbers II. *Mathematics of Computation*, 18, 87–92.

[2] Brillhart, J., & Johnson, G. D. (1960). On the factors of certain Mersenne numbers. *Mathematics of Computation*, 14, 365–369.

[3] Hardy, G. H., & Wright, E. M. (1971). *An Introduction to the Theory of Numbers*. 4th ed. The English Language Book Society.

[4] Kang, S. W. (1989). On the primality of the Mersenne number M_p. *Journal of the Korean Mathematical Society*, 26(1), 75–82.

[5] Kravitz, S. (1961). Divisors of Mersenne numbers $10,000 < p < 15,000$. *Mathematics of Computation*, 15, 292–293.

[6] Leyendekkers, J. V., & Shannon, A. G. (2005). Fermat and Mersenne numbers. *Notes on Number Theory and Discrete Mathematics*, 11(4), 17–24.

[7] Mohanty, S. P., & Ramasamy, A. M. S. (1985). The characteristic number of two simultaneous Pell's equations and its application. *Bulletin of the Belgian Mathematical Society - Simon Stevin*, 59(2), 203–214.

[8] Ramasamy, A. M. S. (2006). Generalized version of the characteristic number of two simultaneous Pell's equations. *The Rocky Mountain Journal of Mathematics*, 36(2), 699–720.

[9] Ribenboim, P. (1996). *The New Book of Prime Number Records*. Springer–Verlag.