Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2024, Volume 30, Number 2, 236–252
DOI: 10.7546/nntdm.2024.30.2.236-252

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

A. M. S. Ramasamy

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

Received: 25 August 2023 **Revised:** 16 March 2024
Accepted: 26 March 2024 **Online First:** 8 May 2024

Abstract: Let ρ be an odd prime ≥ 11. In Part I, starting from an M-cycle in a finite field $\mathbb{F}_\rho$, we have established how the divisors of Mersenne, Fermat and Lehmer numbers arise. The converse question is taken up in this Part with the introduction of an arithmetic function and the notion of a split-associated prime.
Keywords: M-cycle, Jacobi symbol, Arithmetic function, Split-associated prime, Root point.
2020 Mathematics Subject Classification: 11A25, 11A41, 11B50, 11C08, 11T06, 11T30.

1 Introduction

Numbers of the forms $2^n - 1$, $2^n + 1$ and $2^{2^n} + 1$ are referred to as Mersenne, Lehmer and Fermat numbers, respectively. The main purpose of this study is to establish the algebraic principle upon which the factors of these numbers arise. In Part I, [9], the author has introduced the polynomial sequences $\{F_k(x)\}$, $\{G_k(x)\}$ and $\{H_k(x)\}$ over $\mathbb{Z}$ defined as follows:

$$\begin{aligned}
&F_1(x) = x, \;\; F_{k+1}(x) = (F_k(x))^2 - 2, \;\; \forall\, k \in N, \\
&G_0(x) = 1, \;\; G_1(x) = x - 1, G_{k+2}(x) = xG_{k+1}(x) - G_k(x) \;\; (k \geq 0), \\
&H_0(x) = 1, \;\; H_1(x) = x + 1, H_{k+2}(x) = xH_{k+1}(x) - H_k(x) \;\; (k \geq 0).
\end{aligned}$$

In [9], the equivalence of the following statements have been proved:

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

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

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

The concept of satellite polynomial has been introduced.

(i) 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 $p(x) \notin \{G_k(x)\}$.

(ii) 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 $q(x) \notin \{H_k(x)\}$.

With ρ a prime, the values assumed by the sequences in the field $\mathbb{F}_\rho$ have been considered, leading to the sequences $\{M(t)\}$, $\{\theta_{t,k}\}$ and $\{\psi_{t,k}\}$, respectively.

Let ρ be an odd prime ≥ 11. Let $M(t) \in \mathbb{F}_\rho - \{0, \pm 1, \pm 2\}$ such that $M_k^2 \neq 2, 3$ for all 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 positive integer such that $\psi_{t,\omega} = 0$. Then it has been proved in Part I [9], that $\omega \geq n$ and $2\omega + 1 \mid 2^n - 1$ or $2^n + 1$. It has also been proved that $n \mid \frac{1}{2}\Phi(2\omega+1)$.

In Part I, starting from an M-cycle in $\mathbb{F}_\rho$, we have established how the divisors of Mersenne, Fermat and Lehmer numbers arise. The converse question is taken up in this part. One may refer to Brent, Crandall, Dilcher and van Halewyn [1], Brillhart and Johnson [2], Brillhart [3], Gostin [5], Kang [7], Kravitz [8] and Ribenboim [10] for several results on the factors of Mersenne and Fermat numbers. Starting with such a factor, how to find an odd prime ρ and the M-cycle in $\mathbb{F}_\rho$ contributing the factor under consideration? This is the focus of attention in this part.

First we develop the necessary preliminaries and then proceed to settle the converse question. The main results of this study are contained in Theorems 3.2, 3.3, 4.2, 5.10, 6.2, Corollary 6.3 and Theorem 7.3. A summary of results is furnished in Section 8.

2 Classification of M-cycles in the field $\mathbb{F}_\rho$

Consider an M-cycle of length n in the field $\mathbb{F}_\rho$ denoted by $M_1 \to M_2 \to \cdots \to M_n \to M_1 \to \cdots$. Let ω be the corresponding pivotal position in $\mathfrak{C}_1(t)$. In view of [9, Corollary 5.3], $M_1, M_2, \ldots, M_n$ are roots of the polynomial $H_\omega(x)$ over $\mathbb{F}_\rho$. We have the following:

Definition 2.1 (Types of M-cycles)**.** *We say that the M-cycle of length n in $\mathbb{F}_\rho$ is of type I if the M-cycle contributes all the roots of $H_\omega(x)$ and of type II if the elements of the M-cycle form a proper subset of the set of roots of $H_\omega(x)$. i.e., the M-cycle is of type I if $\omega = n$ and of type II if $\omega > n$.*

Example 2.1. *Consider the field $\mathbb{F}_{43}$. Let $(\frac{p}{q})$ denote the Jacobi symbol. We obtain $(\frac{6}{43}) = 1$. It is noted that $36^2 = 1296 \equiv 6 \pmod{43}$. Hence $36^2 - 2 \equiv 4 \pmod{43}$. Choosing $M(t) = 4$, we get the cycle $4 \to 14 \to 22 \to 9 \to 36 \to 4 \to \cdots$ in $\mathbb{F}_{43}$ for which $n = 5$. The Ψ-sequence corresponding to $M(t) = 4$ is $\Psi_{t,0} = 1, \Psi_{t,1} = 5, \Psi_{t,2} = 19, \ldots$, which attains the value of zero at $\omega = 5$. Since $\omega = n$, the M-cycle is of type I.*

Example 2.2. *Take the field* $\mathbb{F}_{1301}$. *We have* $(\frac{36}{1301}) = 1$. *We obtain* $1295^2 = 1677025 \equiv 36 \pmod{1301}$. *Therefore* $1295^2 - 2 \equiv 34 \pmod{1301}$. *Beginning with* $M(t) = 34$, *we get the cycle* $34 \to 1154 \to 791 \to 1199 \to 1295 \to 34 \to \cdots$ *in* $\mathbb{F}_{1301}$ *for which* $n = 5$. *The* Ψ*-sequence corresponding to* $M(t) = 34$ *is* $\Psi_{t,0} = 1$, $\Psi_{t,1} = 35$, $\Psi_{t,2} = 1189, \ldots$, *which attains the value of zero at* $\omega = 15$. *As* $\omega > n$, *the* M*-cycle is of type II.*

Example 2.3. *Consider the field* $\mathbb{F}_\rho$ *with* $\rho = 139$. *We note that* $(\frac{16}{139}) = 1$. *On computation, we get* $135^2 = 18225 \equiv 16 \pmod{139}$. *Consequently* $135^2 - 2 \equiv 14 \pmod{139}$. *Choosing* $M(t) = 14$, *we obtain the cycle* $14 \to 55 \to 104 \to 111 \to 87 \to 61 \to 105 \to 42 \to 94 \to 77 \to 89 \to 135 \to 14 \to \cdots$ *in* $\mathbb{F}_\rho$ *of length* 12. *The* Ψ*-sequence corresponding to* $M(t) = 14$ *is* $\Psi_{t,0} = 1$, $\Psi_{t,1} = 15$, $\Psi_{t,2} = 70, \ldots$, *which attains the value of zero at* $\omega = 17$. *Since* $\omega > n$, *the* M*-cycle is of type II.*

Remark 2.1. *The polynomial satisfied by the elements of the* M*-cycle is a satellite polynomial of* $H_\omega(x)$ *in Example 2.2, as well as Example 2.3.*

Theorem 2.1. *If there is an* M*-cycle of type I in* $\mathbb{F}_\rho$, *then* $2\omega + 1$ *is necessarily a prime.*

Proof. If possible, suppose $2\omega + 1$ is composite. Let $2d + 1$ be a proper divisor of $2\omega + 1$. Then by [9, Theorems 2.12 and 2.15] we have

$$H_\omega(x) = H_d(x)p(x), \tag{2.1}$$

where $H_d(x) \in \{H_k(x)\}$ and $p(x) \notin \{H_k(x)\}$ and they are non-trivial polynomials over $\mathbb{Z}$. Since the degree of $p(x)$ is less than the degree of $H_\omega(x)$, not all the roots of $H_\omega(x)$ in $\mathbb{F}_\rho$ can be roots of $p(x)$. Therefore, there is at least one root of $H_\omega(x)$ in $\mathbb{F}_\rho$ which also satisfies $H_d(x)$. Since $\omega = n$, all the roots of $H_\omega(x)$ are the elements of an M-cycle. Hence $H_d(M(t)) = 0$ for some $M(t) \in \mathbb{F}_\rho$. However, since $H_d(x)$ is an element of the sequence $\{H_k(x)\}$, from [9, Theorem 6.1] it is seen that all the other elements in the M-cycle also satisfy $H_d(x)$. Consequently, we have the degree of $H_d(x)$ equals the degree of $H_\omega(x)$. This implies that degree of $p(x) = 0$, which is a contradiction. □

Remark 2.2. *The converse of the above theorem, however, does not hold as noted in Example 2.2.*

Theorem 2.2. *If the cycle* $M_1 \to M_2 \to \cdots \to M_n$ *is of type I in* $\mathbb{F}_\rho$, *then*

$$\sum_{i=1}^{n} M_i \equiv -1 \pmod{\rho}. \tag{2.2}$$

Proof. By assumption, $\omega = n$. Hence, the polynomial $H_\omega(x)$ has degree n. The coefficients of x^n and x^{n-1} in $H_\omega(x)$ are both 1. Since $M_1, M_2, \ldots, M_n$ exhaust all the roots of $H_\omega(x)$, it follows from the theory of equations that $\sum_{i=1}^{n} M_i \equiv -1 \pmod{\rho}$. □

3 Classification of prime numbers in relation to $G(x)$ and $H(x)$-sequences

A result provided by [9, Theorems 2.12 and 2.14] is the distinction between odd primes and odd composite numbers in the context of the polynomial sequences $\{G_k(x)\}$ and $\{H_k(x)\}$. While considering the polynomials $G_m(x)$ and $H_m(x)$, we have to distinguish between the following two cases:

(i) $2m+1$ is a composite number, and

(ii) $2m+1$ is a prime number.

The first case has already been considered in [9, Section 2]. Now let us consider the case when $2m+1$ is a prime number. A few definitions become imperative in this context. The concept of a satellite polynomial has been introduced in [9, Section 2, Subsection 7]. By [9, Definition 3.9], when an M-cycle is considered in the field $\mathbb{F}_\rho$, we refer to ρ as the background prime. It has been proved in [9, Theorem 6.1] that the elements of an M-cycle are the roots of some $H(x)$-polynomial. In this regard, we have the following classification of prime numbers.

Definition 3.1 (Split-associated prime)**.** *If $2m+1$ is a prime and if $H_m(x)$ has a satellite polynomial $\in \mathbb{F}_\rho[x]$ whose roots are in $\mathbb{F}_\rho$ for some background prime ρ, then $2m+1$ is called a split-associated prime.*

If $2m+1$ is a prime and if $H_m(x)$ has a satellite polynomial $\in \mathbb{F}_\rho[x]$, then it follows that all the proper factors of $H_m(x)$ are satellite polynomials.

Definition 3.2 (Non-split-associated prime)**.** *If $2m+1$ is a prime and if $H_m(x)$ does not have a satellite polynomial $\in \mathbb{F}_\rho[x]$ where ρ is a background prime for $2m+1$, then $2m+1$ is called a non-split-associated prime.*

Definition 3.3 (Universal satellite polynomial)**.** *A satellite polynomial of $H_m(x)$, when it exists, is said to be universal if it is the same irrespective of the background prime under consideration.*

Example 3.1. *The polynomial $p(x) = x^4 - x^3 - 4x^2 + 4x + 1$ is a factor of $H_7(x)$, whatever be the background prime, and it is not in $\{H_k(x)\}$. Hence, $p(x)$ is a universal satellite polynomial for $H_7(x)$.*

Definition 3.4 (Local satellite polynomial)**.** *A satellite polynomial of $H_m(x)$, when it exists, is said to be local, if it takes different expressions depending on the background prime under consideration.*

Example 3.2. *The field $\mathbb{F}_{61}$ possesses the M-cycles $10 \to 37 \to 25 \to 13 \to 45 \to 10 \to \cdots$, $12 \to 20 \to 32 \to 46 \to 40 \to 12 \to \cdots$ and $23 \to 39 \to 55 \to 34 \to 56 \to 23 \to \cdots$, such that the corresponding ω-value for each element of these cycles is 15. It is seen that the field $\mathbb{F}_{311}$ contains the M-cycles $10 \to 98 \to 272 \to 275 \to 50 \to 10 \to \cdots$, $28 \to 160 \to 96 \to 195 \to 81 \to 28 \to \cdots$ and $37 \to 123 \to 199 \to 102 \to 139 \to 37 \to \cdots$, such that the corresponding ω-value for each element of these cycles is also 15.*

As a result, $H_{15}(x)$ *factorizes as* $(x^5-8x^4+23x^3-9x^2+54x-1)(x^5-28x^4+7x^3-26x^2+46x-1)(x^5-24x^4+27x^3-18x^2+14x-1)$ *and* $(x^5-83x^4+288x^3-80x^2+185x-1)(x^5-249x^4+82x^3-99x^2+265x-1)(x^5-289x^4+248x^3-124x^2+164x-1)$ *in* $\mathbb{F}_{61}$ *and* $\mathbb{F}_{311}$*, respectively. Thus, the coefficients of the factors of* $H_{15}(x)$ *depend on the concerned background primes. Consequently, the satellite polynomials of* $H_{15}(x)$ *are local, whenever they exist in some field* $\mathbb{F}_\rho$*. It follows that* 31 *is a split-associated prime.*

Theorem 3.1. *A necessary condition for a prime* p *to be split-associated is that* $\frac{p-1}{2}$ *is composite, but not conversely.*

That the converse does not hold is illustrated by the following example.

Consider the prime $p = 37$. A background prime for p is 149. The following M-cycle exists in $\mathbb{F}_{149}$: $7 \to 47 \to 121 \to 37 \to 26 \to 78 \to 122 \to 131 \to 24 \to 127 \to 35 \to 31 \to 65 \to 51 \to 66 \to 33 \to 44 \to 146 \to 7 \to \cdots$.

For this cycle, $\omega = 18$. Since $\omega = n$, it follows that p is non-split-associated. However, $\frac{p-1}{2}$ is composite.

Theorem 3.2. *If* $2\omega+1$ *is a prime and if* $H_\omega(x)$ *splits into satellite polynomials in* $\mathbb{F}_\rho[x]$*, then all the resulting factors of* $H_\omega(x)$ *are of equal degree.*

Proof. If there are two factors of $H_\omega(x)$ in $\mathbb{F}_\rho[x]$, of degrees n_1 and n_2, respectively, then by [9, Theorem 8.2] we have $2\omega+1 \mid 2^{n_1}-1$ and $2\omega+1 \mid 2^{n_2}-1$ or $2\omega+1 \mid 2^{n_1}+1$ and $2\omega+1 \mid 2^{n_2}+1$.

Since the divisibility by $2\omega+1$ is associated with the smallest n occurring as an exponent in 2^n-1 or 2^n+1, it follows that $n_1 = n_2$. A similar argument applies to the case of the occurrence of several satellite polynomials as factors of $H_\omega(x)$ in $\mathbb{F}_\rho[x]$. □

Employing a similar argument as in the above theorem, we have the following two theorems.

Theorem 3.3. *Let* ρ *and* ρ' *be two background primes for a prime* $2\omega+1$*. If* $H_\omega(x)$ *splits into satellite polynomials, then the satellite polynomials of* $H_\omega(x)$ *in* $\mathbb{F}_\rho[x]$ *and* $\mathbb{F}_(\rho')[x]$ *are of equal degree.*

Theorem 3.4. *If* $2\omega+1$ *is a prime and if* $H_\omega(x)$ *splits into satellite polynomials in* $\mathbb{F}_\rho[x]$*, then all the resulting factors of* $H_\omega(x)$ *are local satellite polynomials.*

Proof. By Theorem 3.2, the resulting factors of $H_\omega(x)$ are of equal degree. Let the degree of any such polynomial be α and let the number of such factors be s. Then the roots of $H_\omega(x)$ in $\mathbb{F}_\rho$ form s number of M-cycles of length α each. Suppose these M-cycles are:

$$\begin{aligned}
&M_{1,1} \to M_{1,2} \to \cdots \to M_{1,\alpha} \to M_{1,1} \to \cdots,\\
&M_{2,1} \to M_{2,2} \to \cdots \to M_{2,\alpha} \to M_{2,1} \to \cdots,\\
&\qquad\qquad \vdots\\
&M_{s,1} \to M_{s,2} \to \cdots \to M_{s,\alpha} \to M_{s,1} \to \cdots.
\end{aligned}$$

For each $i = 1, 2, \ldots s$, let $S_{i,j}$ denote the elementary symmetric functions formed by the elements of the i-th M-cycle, where $j = 1, 2, \ldots, \alpha$. Then

$$H_\omega(x) = \prod_{i=1}^{s} \{x^\alpha - S_{i,1}x^{\alpha-1} + S_{i,2}x^{\alpha-2} - \cdots + (-1)^\alpha S_{i,\alpha}\}. \tag{3.1}$$

Since the $S_{i,j}$'s in (3.1) depend on $\mathbb{F}_\rho[x]$, each factor of $H_\omega(x)$ is a local satellite polynomial. □

Corollary 3.1. *For given $H_\omega(x)$, the degree α of any aforesaid satellite polynomial of $H_\omega(x)$ is unique.*

4 An arithmetic function

Introduction of a new arithmetic function becomes necessary for our study.

Definition 4.1 (Odd part of a natural number)**.** *Define $\delta : N \to N$ as follows: Given a natural number n, we can write $n = 2^\lambda m$, where $\lambda \geq 0$ and m is an odd integer ≥ 1. We define $\delta(1) = 1,\ \delta(2^\lambda) = 1,\ \forall \lambda \geq 1$ and $\delta(2^\lambda m) = m, \forall\ \lambda \geq 0$, provided m is an odd integer. We refer to $\delta(n)$ as the odd part of n.*

We have the following theorem.

Theorem 4.1. *δ is a completely multiplicative function.*

Next we prove a crucial identity involving the arithmetic function δ. The result is contained in the following theorem.

Theorem 4.2 (Property of the function δ)**.** *If α is any odd number ≥ 11, then*

$$\begin{aligned} & \frac{\delta(\alpha-1)-1}{2} + \frac{\delta(\alpha+1)-1}{2} + \left|\frac{\delta(\alpha-1)-1}{2} - \frac{\delta(\alpha+1)-1}{2}\right| \\ = \ & \frac{\alpha - j}{2}, \forall\ \alpha \equiv j \pmod 4, \text{ where } j \in \{1, 3\}. \end{aligned} \tag{4.1}$$

Proof. Case (i): Suppose $\alpha \equiv 1 \pmod 4$. Write $\alpha = 4k + 1$. Then $\frac{\delta(\alpha-1)-1}{2} = \frac{\delta(k)-1}{2}$ and $\frac{\delta(\alpha+1)-1}{2} = k$. If k is odd, then $\delta(k) = k$ and if k is even, then $\delta(k) < k$. Thus in any case, we have $\frac{\delta(k)-1}{2} < k$. Therefore, we get

$$\frac{\delta(\alpha-1)-1}{2} + \frac{\delta(\alpha+1)-1}{2} + \left|\frac{\delta(\alpha-1)-1}{2} - \frac{\delta(\alpha+1)-1}{2}\right| = 2k = \frac{\alpha-1}{2}.$$

Case (ii): Suppose $\alpha \equiv 3 \pmod 4$. Write $\alpha = 4k + 3$. Then $\frac{\delta(\alpha-1)-1}{2} = k$ and $\frac{\delta(\alpha+1)-1}{2} = \frac{\delta(k+1)-1}{2}$. Whether k is odd or even, we have $\frac{\delta(k+1)-1}{2} < k$. Consequently, we obtain

$$\frac{\delta(\alpha-1)-1}{2} + \frac{\delta(\alpha+1)-1}{2} + \left|\frac{\delta(\alpha-1)-1}{2} - \frac{\delta(\alpha+1)-1}{2}\right| = 2k = \frac{\alpha-3}{2}.$$

This completes the proof. □

Corollary 4.1. *There do not exist two distinct primes for which both corresponding odd parts are identical.*

5 Relationship between the pivotal position and the background prime

The concept of pivotal position has been introduced in [9, Definition 5.4]. Suppose ω is the pivotal position in the $\psi_{t,k}$-sequence for an $M(t)$-cycle in $\mathbb{F}_\rho[x]$. In [9, Theorem 5.6], we have proved that 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. Given t, it has been proved in [9, Corollary 5.4] that the period of the cyclic sequence $\theta_{t,k}$ (resp. $\psi_{t,k}$) as a function of k is $2\omega + 1$. On the basis of these results, we establish a relationship between ω and ρ. First we develop the preliminaries.

5.1 The linkage with arithmetic progressions

The role of arithmetic progressions has been brought out in [9, Theorem 2.13]. Further linkage of the pivotal position in the $\psi_{t,k}$-sequence with certain arithmetic progressions is considered in the sequel.

Definition 5.1 (Fundamental arithmetic progression associated with a natural number)**.** *Suppose $n \in N$. An arithmetic progression with first term n and common difference $2n+1$ is called the fundamental arithmetic progression associated with n and is denoted by $S(n)$, i.e., $S(n) = \{n,\ 3n+1,\ 5n+2, \dots\}$.*

Divisibility among odd numbers is transformed into an equivalent problem of arithmetic progressions as follows:

Theorem 5.1. *Suppose $j, m \in N$ with $j < m$. Then $2j+1 \mid 2m+1$ if and only if $S(m) \subset S(j)$.*

Proof. Suppose $2j+1 \mid 2m+1$. Then we have $m \equiv j \pmod{2j+1}$. Hence $m = j + s(2j+1)$ for some $s \in N$. Consequently, $m \in S(j)$. In $S(m)$, any element greater than m is of the form $m + s'(2m+1)$ for some $s' \in N$. Therefore $S(m) \subset S(j)$, proving the if part. A similar proof applies for the converse. □

Corollary 5.1. *If $2m+1 = p^t$ where p is a prime, then*

$$S(m) = S(\frac{p^t-1}{2}) \subset S(\frac{p^{t-1}-1}{2}) \subset \cdots \subset S(\frac{p^2-1}{2}) \subset S(\frac{p-1}{2}).$$

Corollary 5.2. *If $2m+1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ where $p_1, p_2, \dots, p_t$ are distinct primes, then*

$$S(m) = S(\frac{p_1^{\alpha_1}-1}{2}) \cap S(\frac{p_2^{\alpha_2}-1}{2}) \cap \cdots \cap S(\frac{p_t^{\alpha_t}-1}{2}).$$

5.2 Root points

We consider the positions in the second row of the matrix $\mathfrak{a}(M(t))$ at which the $\psi_{t,k}$-sequence attains a zero with $k \geq \rho$. First we have the following theorem.

Theorem 5.2. *Suppose a polynomial $H(x)$-sequence attains a root at ω in the second row of the principal compartment $\mathfrak{C}_1(t)$ of the matrix $\mathfrak{a}(M(t))$. Then the positions in the second row of $\mathfrak{a}(M(t))$ at which the polynomial attains a root are precisely the elements of $S(\omega)$.*

Proof. When the $\psi_{t,k}$-sequence attains a zero at $k = \omega$, by [9, Corollary 5.4] the next zero of the sequence occurs at $k = 3\omega + 1$. The proof is completed by a repetition of this argument. □

Let us find the smallest non-negative integer h such that whenever the $\psi_{t,k}$-sequence contains a root of $H_\omega(x)$ in the field $\mathbb{F}_\rho$, it contains all the roots of $H_\omega(x)$ in $\mathbb{F}_\rho$ at $\psi_{t,k}$ when k takes the value of $\rho + h$.

Definition 5.2 (Root point)**.** *Let ρ be a given odd prime. Suppose $\omega \in N$. The root point of ρ with respect to ω, if it exists, is denoted by $r(\rho, \omega)$ and is defined as the least natural number ρ + h where h is the least non-negative integer such that $H_\omega(x)$ attains all of its ω roots in $\mathbb{F}_\rho$ at $\psi_{t,k}$ with*

$$k = \rho + h. \tag{5.1}$$

If the root point of ρ with respect to ω does not exist, then we say that $r(\rho, \omega)$ is undefined.

Theorem 5.3. *The value of h in* (5.1) *is* 0 *or else* $1 \leq h \leq 2\omega$.

Proof. From [9, Corollary 5.4], it is seen that the roots of $H_\omega(x)$ are attained in the $\psi_{t,k}$-sequence at regular intervals of $2\omega + 1$. Hence the result. □

5.3 Properties of the root points

We consider the derivation of a formula for $r(\rho, \omega)$, when it exists, in terms of ρ and ω. For this purpose we establish certain properties of $r(\rho, \omega)$.

Theorem 5.4. *If $r(\rho, \omega)$ exists, then $r(\rho, \omega) \in S(\omega)$.*

Proof. Follows from Theorem 5.2. □

As a consequence of Theorem 5.4, we refer to $r(\rho, \omega)$ as the root point of ρ in $S(\omega)$.

Example 5.1. *Let us consider $r(307, 38)$. The M-cycles $63 \to 283 \to 267 \to 63 \to \cdots$ and $47 \to 58 \to 292 \to 223 \to 300 \to 47 \to \cdots$ contribute the roots of $H_3(x)$ and $H_5(x)$, respectively in $\mathbb{F}_{307}$. The M-cycle $14 \to 194 \to 180 \to 163 \to 165 \to 207 \to 174 \to 188 \to 37 \to 139 \to 285 \to 175 \to 230 \to 94 \to 238 \to 154 \to 75 \to 97 \to 197 \to 125 \to 273 \to 233 \to 255 \to 246 \to 35 \to 302 \to 23 \to 220 \to 199 \to 303 \to 14 \to \cdots$ contributes 30 roots of $H_{38}(x)$ in $\mathbb{F}_{307}$. Since 7 and 11 are divisors of 77, all the roots of $H_3(x)$ and $H_5(x)$ are also roots of $H_{38}(x)$. Consequently $H_{38}(x)$ has all of its roots in $\mathbb{F}_{307}$ and so $r(307, 38)$ exists. By Corollary 5.2, we have $S(38) = S(3) \cap S(5)$. Using Theorem 5.4, we obtain $r(307, 38) = 346$.*

Notation. Let $\mathfrak{C}_i(t, \rho, \omega)$ $(i = 1, 2, 3, \ldots)$ denote the i-th compartment in the matrix $\mathfrak{a}(t)$ corresponding to the occurrence of the roots of the polynomial $H_\omega(x)$ in $\mathbb{F}_\rho[x]$. The cells in each row of $\mathfrak{a}(t)$ are numbered $0, 1, 2, \ldots$. Let us call these numbers as the indices of the corresponding cells. We have the following crucial result.

Theorem 5.5. *Suppose* $2\omega+1=(2\omega_1+1)(2\omega_2+1)$ *where* $2\omega_1+1$ *and* $2\omega_2+1$ *are primes with* $\omega_1<\omega_2$. *If* $H_\omega(x)$ *attains all of its roots in* $\mathbb{F}_\rho$ *and if* $r(\rho,\omega_1)=\rho+h_1$, $r(\rho,\omega_2)=\rho+h_2$, $r(\rho,\omega)=\rho+h$, *then* $h_1<h_2<h$.

Proof. By Corollary 5.2, we have $S(\omega)=S(\omega_1)\cap S(\omega_2)$. The root points of ρ with respect to $\omega_1,\ \omega_2$ and ω imply that $t_1,t_2,t\in N$ such that $\rho+h_1=\omega_1+t_1(2\omega_1+1), \rho+h_2=\omega_2+t_2(2\omega_2+1), \rho+h=\omega+t(2\omega+1)$.

We have $\psi_{t,\rho+h}=0$, $\psi_{t,\rho+h_1}=0$, $\psi_{t,\rho+h_2}=0$. By assumption, $H_{\omega_1}(x)\mid H_\omega(x)$ and $H_{\omega_2}(x)\mid H_\omega(x)$. Therefore, all the roots of $H_{\omega_1}(x)$ and $H_{\omega_2}(x)$ in $\mathbb{F}_\rho[x]$ are also roots of $H_\omega(x)$. Since $H_\omega(x)$ attains all of its roots at $\psi_{t,k}$ with $k=\rho+h$, it follows that $H_{\omega_1}(x)$ and $H_{\omega_2}(x)$ also attain all of their roots at $\psi_{t,k}$. Consequently, we have $h_1\le h$ and $h_2\le h$. Let $s\in N$ such that $\mathfrak{C}_{s+1}(t,\rho,\omega)$ is the compartment in $\mathfrak{a}(t)$ corresponding to which ρ is the index of a cell. The total number of cells covered by the compartments $\mathfrak{C}_i(t,\rho,\omega)$ $(i=1,2,\ldots,s)$ would have also been covered by the compartments corresponding to ω_1 and ω_2. The number of compartments that are completed in the $\psi_{t,k}$-sequence before the occurrence of $r(\rho,\omega_1)$ is $2(2\omega_2+1)$ while it is $2(2\omega_1+1)$ and 2 for $r(\rho,\omega_2)$ and $r(\rho,\omega)$, respectively. Thus $s=2$. The index of the last cell in the last completed compartment in each case is $2(2\omega_2+1)(2\omega_1+1)-1$. Thus there are equal number of cells in the compartments completed in the $\psi_{t,k}$-sequence before the occurrence of any one of $r(\rho,\omega_1), r(\rho,\omega_2)$ and $r(\rho,\omega)$ and the root points $r(\rho,\omega_1), r(\rho,\omega_2)$ and $r(\rho,\omega)$ occur in the immediate next cell in the $\psi_{t,k}$-sequence. Since $\omega_1<\omega_2$, it is seen that the cells in the $\psi_{t,k}$-sequence of $\mathfrak{C}_{s+1}(t,\rho,\omega)$ containing the roots of $H_{\omega_1}(x),\ H_{\omega_2}(x)$ and $H_\omega(x)$ occur in this order. Hence we have $r(\rho,\omega_1)<r(\rho,\omega_2)<r(\rho,\omega)$. From this relation we conclude that $h_1<h_2<h$. □

Corollary 5.3. *Suppose*

$$2\omega+1=(2\omega_1+1)(2\omega_2+1)\cdots(2\omega_u+1),$$

where $2\omega_1+1, 2\omega_2+1,\ldots,2\omega_u+1$ *are primes with* $\omega_1<\omega_2<\cdots<\omega_u$. *If* $H_\omega(x)$ *attains all of its roots in* $\mathbb{F}_\rho$ *and if* $r(\rho,\omega_1)=\rho+h_1, r(\rho,\omega_2)=\rho+h_2,\ldots,r(\rho,\omega_u)=\rho+h_u, r(\rho,\omega)=\rho+h$, *then* $h_1<h_2<\cdots<h_u<h$.

Next we establish an important condition for the polynomial $H_\omega(x)$ to attain roots in two different finite fields.

Theorem 5.6. *If* ρ *and* ρ' *are primes with* $\rho'>\rho$ *and* $\rho'\equiv\rho\pmod{2\omega+1}$ *and if* $\mathrm{H}_\omega(x)$ *attains all of its roots in both the fields* $\mathbb{F}_\rho$ *and* $\mathbb{F}_{\rho'}$, *then* $r(\rho',\omega)-r(\rho,\omega)=\rho'-\rho$.

Proof. Let us take $r(\rho,\omega)=\rho+h$ and $r(\rho',\omega)=\rho'+h'$. By Theorem 5.3, we have $h=0$ or else $0<h<2\omega+1$ and $h'=0$ or else $0<h'<2\omega+1$. Since ρ and ρ' are odd, it follows that $\rho'\equiv\rho\,(\mathrm{mod}\ 2(2\omega+1))$. The sequence $\Psi_{t,k}$ attains a zero at $k=r(\rho,\omega)$. The next two positions in the $\Psi_{t,k}$-sequence where it attains zeros in $\mathbb{F}_\rho$ are $r(\rho,\omega)+2\omega+1$ and $r(\rho,\omega)+2(2\omega+1)$, respectively.

Let $s\in N$ such that $\mathfrak{C}_{s+1}(t,\rho,\omega)$ is the compartment in $\mathfrak{a}(t)$ corresponding to which ρ is the index of the cell. The index of the last cell in the completed compartments before the occurrence

of ρ as the index of a cell is $s(2\omega+1)-1$. The cells with indices ρ and $\rho+h$ occur in the immediate next compartment.

Let $s' \in N$ such that $\mathfrak{C}_{s'+1}(t,\rho,\omega)$ is the compartment in $\mathfrak{a}(t)$ corresponding to which ρ' is the index of a cell. The cells with indices ρ' and $\rho'+h'$ occur in the immediate next compartment.

Let us consider the forward movement along the $\psi_{t,k}$-sequence from the s-th compartment to $(s'+1)$-st compartment. Since $\rho' \equiv \rho \pmod{2\omega+1}$, the number of cells from the leftmost cell in the $(s+1)$-st compartment to the cell with index ρ is the same as the number of cells from the leftmost cell in the $(s'+1)$-st compartment to the cell with index ρ'. Since a root of $H_\omega(x)$ occurs after h positions from ρ in the $\psi_{t,k}$-sequence and the roots of $H_\omega(x)$ are attained in the $\psi_{t,k}$-sequence at regular intervals of $2\omega+1$, it follows that a root of $H_\omega(x)$ occurs after h positions from ρ' in the $\psi_{t,k}$-sequence. Since h' is the least non-negative integer such that $H_\omega(x)$ attains all of its ω roots in $\mathbb{F}_{\rho'}$ at $\psi_{t,k}$ where $k = \rho' + h'$, it follows that $h' \leq h$. Similarly, considering the backward movement along the $\psi_{t,k}$-sequence from the $(s'+1)$-st compartment to $(s+1)$-st compartment, it is seen that $h \leq h'$. Hence we obtain $h' = h$. Consequently, $r(\rho',\omega) - r(\rho,\omega) = \rho' - \rho$. □

Corollary 5.4. *If ρ and ρ' are primes as in Theorem 5.6, then we have*

$$r(\rho',\omega) \equiv r(\rho,\omega) \pmod{2(2\omega+1)}.$$

Theorem 5.7. *Suppose $t \in N,\ t \geq 2$. Let $2\omega_1+1$ be a prime and $2\omega_t+1 = (2\omega_1+1)^t$. If $H_{\omega_t}(x)$ attains all of its roots in $\mathbb{F}_\rho$ and if $r(\rho,\omega_1) = \rho + h_1, r(\rho,\omega_t) = \rho + h_t$, then $r(\rho,\omega_{i+2}) - r(\rho,\omega_{i+1}) = \omega_1(2\omega_1+1)^i,\ \forall\, i \geq 0$.*

5.4 Attainment of roots of $H(x)$-polynomial

With the necessary tools having been constructed, we prove a result on the attainment of roots of $H(x)$-polynomial in the field $\mathbb{F}_\rho$ with $\rho \geq 11$. We have to distinguish between two cases:

(i) $3 \mid 2\omega+1$, and

(ii) $3n \mid 2\omega+1$.

Theorem 5.8. *If $3 \mid 2\omega+1$, then a necessary condition for $H_\omega(x)$ to attain all of its roots in a field $\mathbb{F}_\rho$ is that $2\omega+1 \mid \delta(\rho-1)$ or $\delta(\rho+1)$.*

Proof. Suppose $2\omega+1 = (2d_1+1)(2d_2+1)$ with $d_1 < d_2$. Then $\omega = 2d_1d_2 + d_1 + d_2$. Suppose $r(\rho,d_1) = \rho + h_1,\ r(\rho,d_2) = \rho + h_2$ and $r(\rho,\omega) = \rho + h$. Then we have $r(\rho,d_1) = d_1 + 2(2\omega+1),\ r(\rho,d_2) = d_2 + 2(2\omega+1)$ and $r(\rho,\omega) = \omega + 2(2\omega+1)$. Consequently,

$$h_2 - h_1 = d_2 - d_1. \tag{5.2}$$

This implies that $h_1 = d_1+1$ if and only if $h_2 = d_2+1$ and $h_1 = d_1-1$ if and only if $h_2 = d_2-1$.

Now consider the assumption that $3 \mid 2\omega+1$. Let us take $d_1 = 1$. Then $h_1 = 0$ or 2. Consequently, $h_2 = d_2+1$ or d_2-1. Hence the theorem. □

Theorem 5.9. *Suppose* $3 \nmid 2\omega + 1$ *and* $H_\omega(x)$ *attains all of its roots in a field* $\mathbb{F}_\rho$. *Suppose* $2\omega' + 1 = 3(2\omega + 1)$. *If* $H_{\omega'}(x)$ *attains all of its roots in some field* $\mathbb{F}_{\rho'}$ *then* $2\omega + 1 \mid \delta(\rho - 1)$ *or* $\delta(\rho + 1)$.

Proof. Suppose $r(\rho, \omega) = \rho + h$ and $r(\rho', \omega') = \rho' + h'$. By Corollary 5.4, we have $r(\rho', \omega) \equiv r(\rho, \omega) \pmod{2(2\omega + 1)}$. Hence $r(\rho, \omega) = \rho' + h'$. By Theorem 5.8, the result holds for $H_{\omega'}(x)$ when $2\omega' + 1$ is a multiple of 3. Hence $2\omega' + 1 \mid \delta(\rho' - 1)$ or $\delta(\rho' + 1)$. This implies that $2\omega + 1 \mid \delta(\rho' - 1)$ or $\delta(\rho' + 1)$. Hence $h' = d_1 + 1$ or $d_1 - 1$. Consequently we obtain $h = d_1 + 1$ or $d_1 - 1$. Thus the theorem holds for $H_\omega(x)$. □

Combining Theorems 5.8 and 5.9, we obtain the following condition for the attainment of all the roots of a $H(x)$-polynomial.

Theorem 5.10. *Let* ρ *be any given odd prime* $\rho \geq 11$. *A necessary condition for* $H_\omega(x)$ *to attain all of its roots in* $\mathbb{F}_\rho$ *is that* $2\omega + 1 \mid \delta(\rho - 1)$ *or* $\delta(\rho + 1)$.

6 Full complement of the roots of polynomials of $H(x)$-sequence

The results in this section come as offshoots of Theorem 4.2. We find an answer to the converse problem emanating from the result contained in Theorem 5.10.

6.1 Existence of non-singular M-cycles in the field $\mathbb{F}_\rho$

Let ρ be a given prime ≥ 11. In the ordered pair (n, ω) with $n, \omega \in N$, let n denote the length of an M-cycle in a field $\mathbb{F}_\rho$ and ω denote the pivotal position in $\mathfrak{C}_1(t)$ at which the $\psi_{t,k}$-sequence attains a zero. We have established in Section 5 that $2\omega + 1 \mid \delta(\rho - 1)$ or $\delta(\rho + 1)$. Because of this property, the M-cycles in $\mathbb{F}_\rho$ can be put in the following two disjoint classes:

(i) M-cycles associated with $\delta(\rho - 1)$, and

(ii) M-cycles associated with $\delta(\rho + 1)$.

If ρ is of the form $2^\tau - 1$, then $\delta(\rho + 1) = 1$. This implies that $\delta(\rho - 1)$ attains the maximum possible value and so all the M-cycles in $\mathbb{F}_\rho$ are associated with $\delta(\rho - 1)$. Similarly, if ρ is of the form $2^\tau + 1$, then all the M-cycles in $\mathbb{F}_\rho$ are associated with $\delta(\rho + 1)$.

Theorem 6.1. *If* ρ *is not of the form* $2^\tau - 1$ *or* $2^\tau + 1$, *then there exist at least two non-trivial* M*-cycles in* $\mathbb{F}_\rho$ *whose corresponding* ω *values are such that* $2\omega + 1 \,|\, \delta(\rho - 1)$ *and* $\delta(\rho + 1)$, *respectively.*

Proof. The existence of at least one non-trivial M-cycle in $\mathbb{F}_\rho$ has been established in [9, Theorem 3.4]. One of $\delta(\rho - 1),\ \delta(\rho + 1)$ has a minimum value of 3 whereas the other one gets a minimum value of 5 with $\gcd(\delta(\rho - 1), \delta(\rho + 1)) = 1$. This implies that $\left| \frac{\delta(\rho-1)-1}{2} - \frac{\delta(\rho+1)-1}{2} \right| \geq 1$. Invoking the identity provided by Theorem 4.2, it is seen that $\frac{\delta(\rho-1)-1}{2} < \frac{\rho-j}{2}$ and $\frac{\delta(\rho+1)-1}{2} < \frac{\rho-j}{2}$

where $j \in \{1, 3\}$ and $j \equiv \rho \pmod 4$. This implies that neither $\frac{\delta(\alpha-1)-1}{2}$ nor $\frac{\delta(\alpha+1)-1}{2}$ attains the maximum possible value. Therefore while it may be the case that several non-trivial M-cycles in $\mathbb{F}_\rho$ are associated with $\delta(\rho-1)$, at least one non-trivial M-cycle is associated with $\delta(\rho+1)$ and vice versa. Hence the theorem. □

Corollary 6.1. *If ρ is not of the form $2^\tau - 1$ or $2^\tau + 1$, then each one of the polynomials $H_{\frac{\delta(\rho-1)-1}{2}}(x)$ and $H_{\frac{\delta(\rho+1)-1}{2}}(x)$ attains at least two roots in $\mathbb{F}_\rho$.*

Proof. Follows from [9, Theorem 6.1] and Theorem 6.1. □

In Definition 3.9 of [9], the concept of background prime for the M-cycle has been introduced.

Definition 6.1 (Minimum background prime)**.** *Given $2\omega + 1 \in N$, the least among all the background primes of $2\omega + 1$ is called the minimum background prime for $2\omega + 1$.*

Certain primes are named after Sophie Germain (1776–1831).

Definition 6.2 (Sophie Germain and safe primes)**.** *A prime p is said to be Sophie Germain if $2p+1$ is also a prime (see for e.g., Ribenboim* [10]*, Roberts* [11] *and Shanks* [12]*). An odd prime p is called a safe prime if $\frac{p-1}{2}$ is also a prime.*

Large Sophie German primes were determined by Dubner [4]. The distribution of these primes was studied by Yates in [13].

An important property possessed by any odd prime ρ in respect of the roots of $H(x)$-polynomials is obtained in the following theorem.

Theorem 6.2 (Existence of full complement of the roots of $H_\omega(x)$)**.** *If ρ is an odd prime ≥ 11 and if $2\omega + 1 \mid \delta(\rho-1)$ or $\delta(\rho+1)$, then the polynomial $H_\omega(x)$ attains all of its roots in $\mathbb{F}_\rho$.*

Proof. We give a proof by induction on ω. First we prove the result for the minimum background prime for $2\omega + 1$ and then extend it to a general background prime for $2\omega + 1$.

When $\omega = 1$, we have the M-cycle $-1 \to -1 \to -1 \to \cdots$, which contributes the root viz. -1 of $H_1(x)$. For the case of $\omega = 2$, consider any odd prime $\rho \equiv \pm 1 \pmod{10}$. In this case, $\left(\frac{5}{\rho}\right) = 1$ and so there exists some element $c \in \mathbb{F}_\rho$ such that $c^2 \equiv 5 \pmod \rho$.

Take $M_1 = \frac{c-1}{2}$ where $\frac{1}{2}$ is the multiplicative inverse of 2 in $\mathbb{F}_\rho$. We check that $M_1 \not\equiv 0, \pm 1, \pm 2 \pmod \rho$. We have $M_2 = M_1^2 - 2 \equiv -\frac{c+1}{2} \pmod \rho$ and $M_3 = M_2^2 - 2 \equiv \frac{c-1}{2} \pmod \rho$. Thus we obtain the M-cycle $M_1 \to M_2 \to M_1 \to \cdots$. It is seen that the elements of this cycle are the roots of $H_2(x) = x^2 + x - 1$.

One can check the cases of $\omega = 3$ through 7 by considering the minimum background prime for $2\omega + 1$. In the case of $\omega = 8$, the minimum background prime for $H_8(x)$ is got as 67. In $\mathbb{F}_{67}$, we have the two M-cycles $13 \to 33 \to 15 \to 22 \to 13 \to \cdots$ and $14 \to 60 \to 47 \to 63 \to 14 \to \cdots$ with $\omega = 8$ for each of these cycles. So $H_8(x)$ attains all of its roots in $\mathbb{F}_{67}$. Thus there is a basis for induction on ω.

Assume the theorem for all satellite polynomials of $H(x)$ of degree $< m$ and for all fields $\mathbb{F}_\rho$ where ρ is the minimum background prime for $2\omega + 1$. Now consider $H_m(x)$. Let ρ be the minimum background prime for $2m + 1$. By Theorem 6.1, it follows that $H(x)$ has at least one

root in $\mathbb{F}_\rho$. Starting from this root, we obtain an M-cycle in $\mathbb{F}_\rho$ of length ≥ 2. We have to consider separately two cases viz. when $2m+1$ is: (i) a prime, and (ii) a composite number.

Case (i). $2m+1$ is a prime. We have to consider two sub-cases.

- Sub-case (i) (A). m is a prime. In this case m is a Sophie Germain prime. It is seen that $H_m(x)$ has no satellite polynomial. The result in this case follows from [9, Theorems 2.12 and 6.1].

- Sub-case (i) (B). m is a composite number.

  - Sub-case (i) (B) (I). $2m+1$ is a non-split-associated prime. In this case, $H_m(x)$ has no satellite polynomial and so it attains all of its ω roots in $\mathbb{F}_\rho$.

  - Sub-case (i) (B) (II). $2m+1$ is a split-associated prime. By Theorem 6.1, there exists at least one root of $H_m(x)$ in $\mathbb{F}_\rho$. By [9, Theorem 6.1], starting from one root of$H_m(x)$, we obtain a non-trivial M-cycle in $\mathbb{F}_\rho$ all of whose elements are roots of $H_m(x)$. Let us form a polynomial $\lambda(x)$, using each one of these elements as a root exactly once. By Theorem 3.4, $\lambda(x)$ is a local satellite polynomial of degree ≥ 4 for $H_m(x)$. Now $\mu(x) = \frac{H_m(x)}{\lambda(x)}$ is a satellite polynomial of $H_m(x)$ and $\deg(\mu(x)) = \deg(H_m(x)) - \deg(\lambda(x)) \leq m-4 < m$. By the induction assumption, $\mu(x)$ has all of its roots in $\mathbb{F}_\rho$. Since each root of $\mu(x)$ is also a root of $H_m(x)$, putting together the roots of $\lambda(x)$ and $\mu(x)$ we obtain all the m roots of $H_m(x)$ in $\mathbb{F}_\rho$.

Case (ii). $2m+1$ is composite. In this case, there exists a prime divisor $2j+1$ of $2m+1$. By [9, Theorems 2.12], $H_j(x)$ is a divisor of $H_m(x)$. Since $j < m$, by Case (i), $H_j(x)$ attains all of its roots in $\mathbb{F}_\rho$. Now $\frac{H_m(x)}{H_j(x)}$, being a satellite polynomial of $H_m(x)$ of degree $m-j < m$, attains all of its roots in $\mathbb{F}_\rho$ which in turn implies the result for $H_m(x)$.

Thus the theorem holds in all the sub-cases, in respect of the field $\mathbb{F}_\rho$ where ρ is the minimum background prime for $2\omega+1$. We now extend the proof to all the fields $\mathbb{F}_\eta$ where η is any other background prime for $2\omega+1$ implying $\eta > \rho$.

The elements in $\mathbb{F}_\rho$ which form M-cycles are linked to the quadratic residues in $\mathbb{F}_\rho$. If $2\omega+1$ is associated with $\delta(\rho-1)$ in $\mathbb{F}_\rho$ and $\delta(\eta-1)$ in $\mathbb{F}_\eta$, then considering the number of quadratic residues associated with the odd parts in the concerned fields, it is seen that at least as much quadratic residues are associated with $\delta(\eta-1)$ in $\mathbb{F}_\eta$ as are associated with $\delta(\rho-1)$ in $\mathbb{F}_\rho$. A similar result holds if $2\omega+1$ is associated with $\delta(\rho-1)$ and $\delta(\eta+1)$ or $\delta(\rho+1)$ and $\delta(\eta-1)$, or $\delta(\rho+1)$ and $\delta(\eta+1)$ in the concerned fields. So $\delta(\eta-1)$ (or $\delta(\eta+1)$, as the case may be) is associated with at least ω roots of $H(x)$ in $\mathbb{F}_\eta$. Since the number of roots of $H(x)$ cannot exceed ω, it follows that $H(x)$ has all of its roots in $\mathbb{F}_\eta$. □

Corollary 6.2. *Given an odd prime $\rho \geq 11$, the polynomials $H_{\frac{\delta(\rho-1)-1}{2}}(x)$ and $H_{\frac{\delta(\rho+1)-1}{2}}(x)$ attain all of their roots in $\mathbb{F}_\rho$.*

Proof. Follows from Corollary 6.1 and Theorem 6.2. □

6.2 Consideration of the converse question

Given an M-cycle in a field $\mathbb{F}_\rho$, it follows from [9, Theorem 6.1] and Theorem 5.10 that the corresponding $\psi_{t,k}$-sequence attains a zero at ω in $\mathfrak{C}_1(t)$ such that $2\omega+1$ divides one of $\delta(\rho-1)$, $\delta(\rho+1)$. The converse question is: *Given a divisor $2\omega+1$ of $\delta(\rho-1)$ or $\delta(\rho+1)$, is there an M-cycle in $\mathbb{F}_\rho$ for which the corresponding $\psi_{t,k}$-sequence attains a zero at ω in $\mathfrak{C}_1(t)$?* The answer is in the affirmative. From Theorems 6.1 and 6.2 and Corollary 6.2, we are led to the following corollary.

Corollary 6.3. *Given an odd prime $\rho \geq 11$ and any divisor $2\omega+1$ of $\delta(\rho-1)$ or $\delta(\rho+1)$, the polynomial $H_\omega(x)$ attains all of its roots in $\mathbb{F}_\rho$.*

This establishes the sufficiency of the condition in Theorem 5.10.

Corollary 6.4. *Every satellite polynomial of $H_{\frac{\delta(\rho-1)-1}{2}}(x)$ (respectively, $H_{\frac{\delta(\rho+1)-1}{2}}(x)$) attains all of its roots in $\mathbb{F}_\rho$.*

Remark 6.1. *An important difference between the stationary sequences $2 \to 2 \to 2 \to \cdots$ and $-1 \to -1 \to -1 \to \cdots$ is brought out by Theorem 6.2. The former sequence does not contribute a root of any polynomial in the $H(x)$-sequence. In contrast, as seen in the course of the proof of Theorem 6.2, the latter sequence contributes a root of $H_1(x)$. Further, if $2\omega+1$ is divisible by 3, the latter sequence also satisfies $H_\omega(x)$ along with some other polynomial $\in H(x)$-sequence and a satellite polynomial of $H_\omega(x)$. Because of this distinction, we refer to the former as singular whereas the latter is said to be non-singular.*

7 M-cycles in the field $\mathbb{F}_\rho$ from the divisors of Mersenne and Lehmer numbers

Previously we have seen the role of arithmetic progressions in the method of cyclic sequences in [9, Section 2] and Section 5 of this Part II. Yet another role of arithmetic progressions is brought out in this section.

7.1 Problem to be considered

In Part I, starting from an M-cycle in a field $\mathbb{F}_\rho$, we have seen how the divisors of Mersenne and Lehmer numbers are obtained as established in [9, Theorem 8.2]. In the other direction, now we take up the following question: *Starting from a given divisor of 2^n-1 or 2^n+1, is it possible to obtain a field $\mathbb{F}_\rho$ which contains an M-cycle of length n such that the corresponding $\psi_{t,k}$-sequence attains a zero at ω in the compartment $\mathfrak{C}_1(t)$?*

To answer this question, we consider an application of Dirichlet's theorem on primes in arithmetic progression. Dirichlet (see for e.g., Hardy and Wright [6]) proved the following theorem: *If a is positive and a and b have no common divisor except 1, then there are infinitely many primes of the form $an+b$.*

Employing the above result, we have the following theorem.

Theorem 7.1. *Given $2\omega + 1 \in N$, each one of the sequences $\{2n(2\omega + 1) - 1 \ / \ n \in N\}$ and $\{2n(2\omega + 1) + \ 1 \ / \ n \in N\}$ contains infinitely many primes.*

As a consequence of Theorem 7.1, given $2\omega + 1 \in N$, the existence of infinitely many background primes for $2\omega + 1$ is guaranteed. In Theorem 6.2, it has been proved that the polynomial $H(x)$ attains all of its roots in $\mathbb{F}_\rho$. As a result, starting from a given divisor $2\omega + 1$ of $2^n - 1$ or $2^n + 1$ and choosing any background prime ρ for $2\omega + 1$, we obtain either one M-cycle or several M-cycles in $\mathbb{F}_\rho$ such that all the corresponding $\psi_{t,k}$-sequences attain zeros at $k = \omega$, as shown in [9, Theorem 6.1].

Thus we have proved the following theorem.

Theorem 7.2. *Given any natural number ω, there exist infinitely many background primes ρ for $2\omega + 1$ such that the polynomial $H_\omega(x)$ attains all of its roots in $\mathbb{F}_\rho$.*

We observe that the converse of [9, Theorem 8.2] is established by Corollary 6.3 and Theorem 7.2.

7.2 How do the divisors of Mersenne, Fermat and Lehmer numbers emerge?

From [9, Theorems 6.1 and 8.2] and Theorems 6.2 and 7.2, a complete theory follows as to the emergence of the divisors of Mersenne, Fermat and Lehmer numbers. It is seen that the divisors of Mersenne and Lehmer numbers lead to M-cycle in a field $\mathbb{F}_\rho$. A related question is: *Starting from a given $n \in N$, how to obtain an M-cycle of length n?* For this, we recall the relationship between n and ω in [9, Theorem 8.3], namely $n \mid \frac{1}{2}\Phi(2\omega + 1)$. Given $n \in N$, we select the smallest $\omega \in N$ such that $n \mid \frac{1}{2}\Phi(2\omega + 1)$. Choose an odd prime ρ such that $(2\omega + 1) \mid \rho - 1$ or $\rho + 1$. Then there exists an M-cycle of length n in $\mathbb{F}_\rho$. Thus we have obtained the following theorem.

Theorem 7.3. *If $2\omega + 1$ is a given divisor of a Mersenne or Lehmer or Fermat number, then there exists a background prime ρ for $2\omega + 1$ such that the field $\mathbb{F}_\rho$ contains an M-cycle for which the $\psi_{t,k}$-sequences attain zeros at $k = \omega$.*

Example 7.1. *Suppose that the M-cycle for the divisor 47 of $2^{23} - 1$ is required. We employ Theorem 6.2. For $2\omega + 1 = 47$, we search for a background prime ρ which should be such that $(2\omega + 1) \mid \rho - 1$ or $\rho + 1$. We see that the prime 281 satisfies the required condition. In $\mathbb{F}_{281}$, we obtain the M-cycle $15 \to 223 \to 271 \to 98 \to 48 \to 54 \to 104 \to 136 \to 229 \to 173 \to 141 \to 209 \to 124 \to 200 \to 96 \to 222 \to 107 \to 207 \to 135 \to 239 \to 76 \to 154 \to 110 \to 15 \to \cdots$ of length $n = 23$.*

Example 7.2. *Consider the divisor 59 of $2^{29} + 1$. For $2\omega + 1 = 59$, a background prime ρ is obtained as 353. In $\mathbb{F}_{353}$, we get the M-cycle $7 \to 47 \to 89 \to 153 \to 109 \to 230 \to 301 \to 231 \to 56 \to 310 \to 82 \to 15 \to 223 \to 307 \to 349 \to 14 \to 194 \to 216 \to 58 \to 185 \to 335 \to 322 \to 253 \to 114 \to 286 \to 251 \to 165 \to 42 \to 350 \to 7 \to \cdots$ of length $n = 29$.*

8 Conclusion

Numbers of the forms $2^n - 1, 2^n + 1$ and $2^{2^n} + 1$ are referred to as Mersenne, Lehmer and Fermat numbers, respectively. We consider the following sequences:

$$F_1(x) = x, F_{k+1}(x) = (F_k(x))^2 - 2, \forall\ k \in N,$$
$$G_0(x) = 1, G_1(x) = x - 1, G_{k+2}(x) = xG_{k+1}(x) - G_k(x)\ (k \geq 0),$$
$$H_0(x) = 1, H_1(x) = x + 1, H_{k+2}(x) = xH_{k+1}(x) - H_k(x)\ (k \geq 0).$$

We have proved the following result: Let ρ be an odd prime ≥ 11. Let $M(t) \in \mathbb{F}_\rho - \{0, \pm 1, \pm 2\}$ such that $M_k^2 \neq 2, 3$ for all 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 positive integer such that $\psi_t, \omega = 0$. Then $2\omega + 1 \mid 2^n - 1$ or $2^n + 1$ and $n \mid \frac{1}{2}\Phi(2\omega + 1)$.

The M-cycles are classified as type I and type II and primes are classified as split-associated and non-split-associated. If $2\omega + 1$ is a prime and if $H_\omega(x)$ splits into satellite polynomials in $\mathbb{F}_\rho[x]$, then we have proved that all the resulting factors of $H_\omega(x)$ are of equal degree. If ρ and ρ' are two background primes for a prime $2\omega + 1$ and if $H_\omega(x)$ is split-associated, then we have proved that the satellite polynomials of $H_\omega(x)$ in $\mathbb{F}_\rho[x]$ and $\mathbb{F}_(\rho')[x]$ are of equal degree. The converse question is taken up: *Given the divisors of Mersenne or Lehmer numbers, how to find a field $\mathbb{F}_\rho$ and the M-cycles in $\mathbb{F}_\rho$ which would yield the factors under consideration?* For establishing a relationship between the pivotal position and the background prime, we have employed the concept of root points which enables us to determine the roots of polynomials of $H(x)$-sequence. We have proved the following result: If ρ is an odd prime, a necessary condition for $H_\omega(x)$ to attain all of its roots in $\mathbb{F}_\rho$ is that $2\omega + 1 \mid \delta(\rho - 1)$ or $\delta(\rho + 1)$. Using this result, we are led to M-cycles from the divisors of Mersenne or Lehmer numbers. We have obtained the following result: If ρ is an odd prime ≥ 11 and if $2\omega + 1 \mid \delta(\rho - 1)$ or $\delta(\rho + 1)$, then the polynomial $H(x)$ attains the full complement of roots in $\mathbb{F}_\rho$. This establishes the sufficiency of the condition. Using Dirichlet's theorem on primes in arithmetic progression, we have proved the following theorem: Given any natural number ω, there exist infinitely many background primes ρ for $2\omega + 1$ such that the polynomial $H_\omega(x)$ attains all of its roots in $\mathbb{F}_\rho$.

Acknowledgements

The author is grateful to the reviewers for the suggestions for the improvement of the paper.

References

[1] Brent, R. P., Crandall, R., Dilcher, K., & van Halewyn, C. (2000). Three new factors of Fermat numbers. *Mathematics of Computation*, 69(231), 1297–1304.

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

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

[4] Dubner, H. (1996). Large Sophie Germain primes. *Mathematics of Computation*, 65(213), 393–396.

[5] Gostin, G. B. (1990). New factors of Fermat numbers. *Mathematics of Computation*, 64(209), 393–395.

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

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

[8] Kravitz, S. (1961). Divisors of Mersenne numbers $10,000 < p < 15,000$. *Mathematics of Computation*, 15(75), 292–293.

[9] Ramasamy, A. M. S. (2024). Sequences in finite fields yielding divisors of Mersenne, Fermat and Lehmer numbers, I. *Notes on Number Theory and Discrete Mathematics*, 30(1), 116–140.

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

[11] Roberts, J. (1992). *Lure of the Integers*. The Mathematical Association of America.

[12] Shanks, D. (1978). *Solved and Unsolved Problems in Number Theory* (2nd ed.). Chelsea Publishing Company.

[13] Yates, S. (1991). Sophie Germain primes. In: Rassias, G. M. (ed.) *The Mathematical Heritage of C. F. Gauss*, World Scientific Publication Company, 882–886.