Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2024, Volume 30, Number 4, 755–775
DOI: 10.7546/nntdm.2024.30.4.755-775

Partitions of numbers and the algebraic principle of Mersenne, Fermat and even perfect numbers

A. M. S. Ramasamy

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

Received: 16 June 2024 **Revised:** 13 November 2024
Accepted: 14 November 2024 **Online First:** 14 November 2024

Abstract: Let ρ be an odd prime greater than or equal to 11. In a previous work, starting from an M-cycle in a finite field $\mathbb{F}_\rho$, it has been established how the divisors of Mersenne, Fermat and Lehmer numbers arise. The converse question has been taken up in a succeeding work and starting with a factor of these numbers, a method has been provided to find an odd prime ρ and the M-cycle in $\mathbb{F}_\rho$ contributing the factor under consideration. Continuing the study of the two previous works, a certain type of partition of a natural number is considered in the present paper. Concerning the Mersenne, Fermat and even perfect numbers, the algebraic principle is established.
Keywords: Partition, Different kinds of M-cycles, The functions T and U, Invariants of a natural number, Tests of primality of Mersenne and Fermat numbers.
2020 Mathematics Subject Classification: 11A51, 11B50, 11P81, 11T06.

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 [13], the author has introduced the polynomial sequences $\{F_k(x)\}$, $\{G_k(x)\}$ and $\{H_k(x)\}$ over $\mathbb{Z}$ defined as follows:

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

In [13], it has been proved that the following statements are equivalent:

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

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

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

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 by the author in [13] 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 [13], 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 has been settled in the affirmative in [14]. Starting with a factor of Mersenne, Fermat or Lehmer numbers, a method has been provided in [14] to answer the question as to finding an odd prime ρ and the M-cycle in $\mathbb{F}_\rho$ contributing that factor. Leyendekkers and Shannon [12] have determined some significant aspects of Mersenne and Fermat numbers. In the present study, the theory of partition of a natural number in relation to the polynomial sequence $\{H_k(x)\}$ is developed and applied in the derivation of the algebraic principle of Mersenne, Fermat and even perfect numbers. The main results are contained in Theorems 3.1, 3.3, 4.1, 4.2, Corollary 4.2, Theorems 4.3, 5.1, 5.2, 8.1, 9.3, 9.4, 10.3, 10.4 and 11.1. A summary is furnished in Section 12.

2 Partition of a natural number in relation to $H(x)$-sequence

Attainment of the roots of the $H(x)$-polynomials has been considered in [14, Section 5]. When ρ is an odd prime ≥ 11, it has been proved in [14, Theorem 5.10] that a necessary condition for $H_\omega(x)$ to attain all its roots in the finite field $\mathbb{F}_\rho$ is that $2\omega + 1 \mid \delta(\rho - 1)$ or $\delta(\rho + 1)$. If ρ is an odd prime ≥ 11 and if $2\omega + 1 \mid \delta(\rho - 1)$ or $\delta(\rho + 1)$, then it has been proved in [14, Theorem 6.2] that the polynomial $H_\omega(x)$ attains all its roots in $\mathbb{F}_\rho$, thereby establishing the sufficiency of the condition. The objective of the present study is to show how the case-by-case consideration in [14, Theorem

6.2] leads to the fundamental theorem of partition of a natural number ω in $\mathbb{F}_\rho$. For the theory of partitions, a standard reference is Andrews [1]. In general, a partition function refers to the number of distinct ways of representing a given natural number ω as a sum of numbers less than or equal to ω. In the present work we deal with a specific method of representation of ω related to our theory, by giving a concrete shape to the result contained in [14, Theorem 6.2].

3 Derivation of partition

Let us recall the following results from [14, Theorems 3.2 and 3.3]:

(1) 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.

(2) If ρ and ρ' are two background primes for a prime $2\omega + 1$ and if $H_\omega(x)$ is split-associated, then the satellite polynomials of $H_\omega(x)$ in $\mathbb{F}_\rho[x]$ and $\mathbb{F}_(\rho')[x]$ are of equal degree.

In order to develop the theory of partitions, a few definitions are needed.

Definition 3.1 (Standard polynomial factorization of $H(x)$-polynomial with respect to $\mathbb{F}_\rho$)**.** *Let ρ be a given prime ≥ 11. In the 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 the pivotal position in $\mathfrak{C}_1(t)$ at which the $\psi_{t,k}$- sequence attains a zero in $\mathbb{F}_\rho$. By the fundamental theorem of arithmetic, $2\omega + 1$ can be uniquely expressed as a product of distinct primes $q_1, \dots, q_t$ as*

$$2\omega + 1 = {q_1}^{\gamma_1} \cdots {q_t}^{\gamma_t}. \tag{3.1}$$

where $\gamma_1, \dots, \gamma_t \in N$. By [13, Theorem 2.17] and [14, Theorems 3.2, 3.4 and Corollary 3.1], the polynomial $H_\omega(x)$ can be uniquely expressed as a product of a certain number of elements of the sequence $H_k(x)$ and a certain number of satellite polynomials (universal or local). This expression is called the standard polynomial factorization of $H_\omega(x)$ with respect to the field $\mathbb{F}_\rho$.

3.1 Constituent polynomials and their properties

Definition 3.2 (Constituent polynomials of $H(x)$-polynomial with respect to $\mathbb{F}_\rho$)**.** *The polynomials appearing in the standard polynomial factorization of $H_\omega(x)$ with respect to the field $\mathbb{F}_\rho$ are called the constituent polynomials of $H_\omega(x)$ with respect to $\mathbb{F}_\rho$ and these polynomials together form the set of constituent polynomials of $H_\omega(x)$ with respect to $\mathbb{F}_\rho$.*

Definition 3.3 (Leading constituent polynomial of $H(x)$-polynomial in relation to $\mathbb{F}_\rho$)**.**
A constituent polynomial of $H_\omega(x)$ of the largest degree with respect to $\mathbb{F}_\rho$ is called a leading constituent polynomial of $H_\omega(x)$ in relation to $\mathbb{F}_\rho$.

3.2 Criterion for a partition

A necessary condition for a partition is that the numbers that would appear in the partition of ω shall add to ω. We think of a partition of ω with a criterion that such a partition shall be based on the relationship between n and ω under consideration. The basic principle in the partition of ω is provided by [13, Theorem 6.1] according to which every root of $H_\omega(x)$ is an element of a unique M-cycle in $\mathbb{F}_\rho$ and, in the other direction, every element of an M-cycle in $\mathbb{F}_\rho$ satisfies some polynomial in the $H(x)$-sequence.

Given $\omega \in N$, consider $H_\omega(x)$. Let ρ be the minimum background prime for $2\omega + 1$. In [14, Theorem 5.10], it has been proved that a necessary condition for $H_\omega(x)$ to attain all its roots in $\mathbb{F}_\rho$ is that $2\omega + 1|\delta(\rho - 1)$ or $\delta(\rho + 1)$ and in [14, Theorem 6.2] we have established that if $2\omega + 1$ is any divisor of $\delta(\rho - 1)$ or $\delta(\rho + 1)$, then the polynomial $H(x)$ attains all its roots in $\mathbb{F}_\rho$.

We denote the partition of ω in $\mathbb{F}_\rho$ by $\pi(\omega)$. Invoking [13, Theorem 2.17] and [14, Theorems 3.2, 3.4 and Corollary 3.1], the expression for $\pi(\omega)$ is derived by referring to the lengths of the M-cycles in $\mathbb{F}_\rho$ as described below:

Case (i): $2\omega + 1$ is a prime.

Sub-case (i) (A): ω is a prime. In this case, ω is a Sophie Germain prime. We see that $H(x)$ has no satellite polynomial and therefore all the roots of $H_\omega(x)$ form a single M-cycle of length ω in $\mathbb{F}_\rho$. Consequently, $\pi(\omega)$ is obtained as ω. Let us employ the notation $\pi(\omega) = (\omega)$.

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

- Sub-case (i) (B) (I): $2\omega + 1$ is a non-split-associated prime. In this case also $H_\omega(x)$ has no satellite polynomial and so the roots of H_ω form a single M-cycle in $\mathbb{F}_\rho$. Thus we have $\pi(\omega) = (\omega)$.

- Sub-case (i) (B) (II): $2\omega + 1$ is a split-associated prime. As established in [14, Theorem 3.2] all the resulting factors of $H_\omega(x)$ in $\mathbb{F}_\rho[x]$ are of equal degree. By [14, Theorem 3.4], the polynomial $H(x)$ splits into local satellite polynomials in $\mathbb{F}_\rho[x]$. Suppose $H_\omega(x)$ factors into s number of local satellite polynomials of degree n each so that $\omega = sn$ with $s > 1$. Then correspondingly we have s number of M-cycles in $\mathbb{F}_\rho$ each of length n. For all these M-cycles, the pivotal position in the corresponding $\psi_{t,k}$-sequences is ω. Thus, while any individual M-cycle can contribute only a part of the set of roots of $H_\omega(x)$, all the M-cycles collectively yield the full complement of the roots of $H_\omega(x)$ in $\mathbb{F}_\rho$. Because of this property, we say that the M-cycles are of sharing type. In this case the partition of ω is given by

$$\pi(\omega) = \underbrace{(n + \cdots + n)}_{(s \text{ times})}$$

  with $sn = \omega$ and $s > 1$. The equality of numbers enclosed within parentheses in the expression for $\pi(\omega)$ indicate that all the corresponding M-cycles have the same value of ω in the concerned $\psi_{t,k}$-sequences. Further, each number within parentheses in $\pi(\omega)$ denotes the length of the corresponding M-cycle in $\mathbb{F}_\rho$. Another interpretation is also in order. Each number within parentheses in $\pi(\omega)$ indicates the degree of the polynomial dividing $H_\omega(x)$ wherein the roots form an M-cycle. The number of items within parentheses in $\pi(\omega)$ denotes the number of such polynomials into which the roots of $H_\omega(x)$ split in $\mathbb{F}_\rho$.

Case (ii): $2\omega + 1$ is a composite number.
In this case the partition of ω depends on the nature of the prime factors of $2\omega + 1$, i.e., whether they are split-associated primes or non-split-associated primes. The partition of ω is obtained in various cases as described below.

Suppose $2\omega + 1$ is a product of two distinct primes $2q_1 + 1$ and $2q_2 + 1$. Then $H_\omega(x)$ has a satellite polynomial as a factor and two other factors from the $H(x)$-sequence. So we have in this case

$$\pi\left(\frac{(2q_1 + 1)(2q_2 + 1) - 1}{2}\right) = \pi(2q_1q_2) + \pi(q_1) + \pi(q_2). \tag{3.2}$$

The partition of $2q_1q_2$ in (3.2) depends on whether or not the satellite polynomial $\frac{H_\omega(x)}{H_{q_1}(x)H_{q_2}(x)}$ of $H_\omega(x)$ is again a product of a certain number of satellite polynomials of $H_\omega(x)$, universal or local.

If both $2q_1 + 1$ and $2q_2 + 1$ in (3.2) are non-split-associated primes, then we have $\pi(\omega) = \pi(2q_1q_2) + (q_1) + (q_2)$ where $\pi(2q_1q_2)$ has to be determined.

If one of $2q_1 + 1$ and $2q_2 + 1$ is a split-associated prime or both of them are of this type, we have to continue the procedure by determining the parts of $\pi(q_1)$ or $\pi(q_2)$ as the case may be.

Next suppose $2\omega + 1 = q^2$ where q is a prime. In this case we have

$$\pi\left(\frac{q^2 - 1}{2}\right) = \pi\left(\frac{q(q-1)}{2}\right) + \pi\left(\frac{q-1}{2}\right). \tag{3.3}$$

If q is a non-split-associated prime in (3.3), then we have $\pi(\omega) = \pi(\frac{q(q-1)}{2}) + (\frac{q-1}{2})$. If q is a split-associated prime in (3.3), then we have $\pi(q) = \underbrace{(n + \cdots + n)}_{(s \text{ times})}$, where $sn = q$ and $s > 1$. In either case, $\pi(2q_1q_2)$ has to be computed by considering the concerned satellite polynomials.

Generalizing the procedure outlined above, one is led to the following result.

Theorem 3.1 (Fundamental theorem of partition with respect to the finite field $\mathbb{F}_\rho$)**.** *Let ρ be a given odd prime greater than or equal to 11 and $\omega \in N$ such that $2\omega + 1 \mid \delta(\rho - 1)$ or $\delta(\rho + 1)$. With respect to $\mathbb{F}_\rho$ we have*

$$\pi(\omega) = (n_{1,1} + \cdots + n_{1,s_1}) + \cdots + (n_{r,1} + \cdots + n_{r,s_r}) + (\eta_1) + (\eta_2) + \cdots + (\eta_t) \tag{3.4}$$

with $n_{1,1} = \cdots = n_{1,s_1}, n_{2,1} = \cdots = n_{2,s_2}, \ldots,\ n_{r,1} = \cdots = n_{r,s_r}$.

The numbers $n_{1,1}, \ldots, n_{1,s_1}, \ldots, n_{r,1}, \ldots, n_{r,s_r}, \eta_1, \eta_2, \ldots, \eta_t$ in the right side of (3.4) are called the elements of the partition of ω. The largest number in $\pi(\omega)$ is written in the leftmost position and the other numbers are written in the decreasing order from left to right. Sometimes the expression for $\pi(\omega)$ may consist of just one number. The equality of numbers enclosed within parentheses indicates that all the corresponding $\psi_{t,k}$-sequences have the same pivotal position. A single element enclosed within parentheses gives rise to a divisor of $H_\omega(x)$ which is either an element of the $H(x)$-sequence or a satellite polynomial of $H_\omega(x)$. A satellite polynomial of $H_\omega(x)$, along with other divisors of $H_\omega(x)$, contributes the roots of a polynomial in the $H(x)$-sequence. Each one of the numbers in the right side of (3.4) denotes the length of an M-cycle in $\mathbb{F}_\rho$. Such of those elements of $\mathbb{F}_\rho$ which occur in these M-cycles provide the full complement of the roots of $H_\omega(x)$.

3.3 Interpretation of a partition

The term $\pi(\omega)$ in (3.4) is a representation with respect to $\mathbb{F}_\rho$ of the splitting up of the polynomial $H_\omega(x)$ into a certain number of polynomials which are either in the $H(x)$-sequence or universal or local satellite polynomials of $H_\omega(x)$. Thus the numbers in $\pi(\omega)$ indicate the degrees of the constituent polynomials in the standard polynomial factorization of $H_\omega(x)$ with respect to $\mathbb{F}_\rho$. Equivalently, the partition of a natural number ω in relation to the $H(x)$-sequence represents the decomposition of the set of the full complement of the roots of $H_\omega(x)$ into a certain number of subsets each of which is composed of an M-cycle in $\mathbb{F}_\rho$ and the numbers in $\pi(\omega)$ refer to the lengths of such M-cycles.

Definition 3.4 (Part of a partition)**.** *Each set of numbers enclosed within parentheses in the right side of* (3.4) *forms a part of* $\pi(\omega)$.

Definition 3.5 (Atom)**.** *Each number appearing in the partition of ω is called an atom of ω with respect to ρ. Thus an atom of ω is the degree of a constituent polynomial in the standard polynomial factorization of $H_\omega(x)$ with respect to $\mathbb{F}_\rho$.*

Definition 3.6 (Atom-set)**.** *The numbers appearing in the partition of ω form the atom-set of ω with respect to ρ.*

Definition 3.7 (Types of parts of a partition)**.** *A part of $\pi(\omega)$ with just one atom is called a uni-atom part. A part of $\pi(\omega)$ with two or more atoms is called a multi-atom part.*

It is seen that the parts $(n_{1,1}+\cdots+n_{1,s_1}), (n_{2,1}+\cdots+n_{2,s_2}), \ldots, (n_{r,1}+\cdots+n_{r,s_r})$ in (3.4) are of multi-atom type while $(\eta_1), (\eta_2), \ldots, (\eta_t)$ are of uni-atom type.

3.4 Different kinds of M-cycles

From Theorem 3.1, we observe the following possibilities of different kinds of M-cycles in $\mathbb{F}_\rho$.

Definition 3.8 (Different kinds of M-cycles)**.** *An M-cycle is referred to as a uni-atom cycle (respectively, multi-atom cycle) if the elements of the cycle give rise to a uni-atom part (respectively, multi-atom part) of a partition of a natural number. An M-cycle is said to be autonomous if the full complement of the roots of the corresponding $H(x)$-polynomial is constituted by the atom(s) in the cycle. A multi-atom cycle is said to be of internal sharing type if the elements of the cycle constitute the full complement of the roots of some $H(x)$-polynomial. An M-cycle, whether uni-atom or multi-atom, is said to be of external sharing type if the elements of the cycle together with the elements of some other M-cycle(s) form the full complement of the roots of some $H(x)$-polynomial. Consequently, it is seen that $\pi(\omega)$ may be composed of the elements which form one or several of the following:*

(i) Uni-atom, autonomous cycle,

(ii) Uni-atom, external sharing type cycle,

(iii) Multi-atom, autonomous cycle,

(iv) Multi-atom, external sharing type cycle.

3.5 Number-theoretic functions

It becomes necessary to introduce two number-theoretic functions.

Definition 3.9 (The Functions T and U associated with a partition)**.** *Define $T : N \to N$ and $U : N \to N$ as follows: The largest atom in $\pi(\omega)$ is defined as the leading atom of ω with respect to ρ and is denoted by $T(\omega)$. Thus $T(\omega)$ is the degree of a constituent polynomial of the largest degree occurring in the expression of $H_\omega(x)$ given by Theorem 3.1. The part of $\pi(\omega)$ containing the leading atom of ω is defined as the leading part of $\pi(\omega)$.*
The number of elements in a part in the partition of $\pi(\omega)$ is called the u-value of that part. The number of elements in the leading part of $\pi(\omega)$ is denoted by U(ω). Thus $U(\omega)$ represents the number of M-cycles contained in the leading part of $\pi(\omega)$.

Any finite field $\mathbb{F}_\rho$ contains the cycle $-1 \to -1 \to \cdots$ contributing the root of $H_1(x)$. This gives rise to the partition $\pi(1) = (1)$. Hence $T(1) = 1$ and $U(1) = 1$. If the largest atom in $\pi(\omega)$ is n and if the leading part of $\pi(\omega)$ is (n), then $T(\omega) = n$ and $U(\omega) = 1$. If the leading part of $\pi(\omega)$ is $\underbrace{(n + \cdots + n)}_{(s \text{ times})}$ with $s \in N$ and $s > 1$, then $T(\omega) = n$ and $U(\omega) = s$.

Theorem 3.2. *The number of parts of $\pi(\omega)$ is $d(2\omega + 1) - 1$ where d is the number of divisors function.*

Proof. Each factor > 1 of $2\omega + 1$ contributes a part of $\pi(\omega)$. Hence the result follows. □

Theorem 3.3. *Every atom of ω is a divisor of $T(\omega)$.*

Proof. First let us consider the case when $2\omega + 1$ is a prime p. This breaks into two cases.
Case (i): p is a non-split-associated prime. In this case we have $\pi(\frac{p-1}{2}) = (\frac{p-1}{2})$.
Case (ii): p is a split-associated prime. In this case we have $\pi(\frac{p-1}{2}) = \underbrace{(n + \cdots + n)}_{(s \text{ times})}$ where $sn = \frac{p-1}{2}$ and $s > 1$. Thus the result holds in the above two cases.

Next let us consider the case when $2\omega + 1$ is a composite number. First let us suppose that $2\omega + 1$ is a product of two distinct primes p and q. We have in this case

$$\pi(\frac{pq-1}{2}) = \pi(\frac{(p-1)(q-1)}{2}) + \pi(\frac{p-1}{2}) + \pi(\frac{q-1}{2}).$$

Both $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are divisors of $\frac{(p-1)(q-1)}{2}$. Therefore each atom in $\frac{p-1}{2}$, as well as $\frac{q-1}{2}$ is a divisor of $\frac{(p-1)(q-1)}{2}$. From this observation it follows that each atom in $\frac{p-1}{2}$ (respectively, $\frac{q-1}{2}$) divides $T(\frac{(p-1)(q-1)}{2})$. A similar proof holds when $2\omega + 1$ is the square of a prime. The proof for the remaining cases is completed by induction on the number of positive divisors of $2\omega + 1$. □

Corollary 3.1. *If $2j + 1$ divides $2\omega + 1$, then every atom of j is a divisor of $T(\omega)$.*

Corollary 3.2. *If p is an odd prime and if p divides $2\omega + 1$, then $T(\frac{p-1}{2})$ is a divisor of T(ω).*

Corollary 3.3. *If $2j + 1$ divides $2\omega + 1$, then the expression for $\pi(j)$ is completely contained in that of $\pi(\omega)$.*

Corollary 3.4. *If $T(\omega) = n$, then $2\omega + 1$ divides $2^n + 1$ or $2^n - 1$.*

Proof. Follows from [13, Theorem 8.2]. □

4 Determination of the leading atom

We have the following facts:

- If p is a Sophie Germain prime, then $T(p) = p$.
- If p is a non-split-associated prime, then $T(\frac{p-1}{2}) = \frac{p-1}{2}$.
- If p is a split-associated prime and if $\pi(\frac{p-1}{2}) = \underbrace{(n + \cdots + n)}_{(s \text{ times})}$ where $sn = \frac{p-1}{2}$ and $s > 1$, then $T(\frac{p-1}{2}) = n$.

Extending these facts, we have the following result.

Theorem 4.1. *Let ρ be an odd prime. Suppose p and q are distinct odd primes with pq dividing $\delta(\rho - 1)$ or $\delta(\rho + 1)$. Then*

$$T\left(\frac{pq-1}{2}\right) = j \operatorname{lcm}\left(T(\frac{p-1}{2}), T(\frac{q-1}{2})\right), \ j \in \{1, 2\} \textit{ with respect to } \rho. \tag{4.1}$$

Proof. Denote $\operatorname{lcm}\left(T\left(\frac{p-1}{2}\right), T\left(\frac{q-1}{2}\right)\right)$ by α. By Corollary 3.1, it follows that $T\left(\frac{p-1}{2}\right)$ and $T\left(\frac{q-1}{2}\right) \mid T\left(\frac{pq-1}{2}\right)$. Hence, p and q are divisors of $2^\alpha + 1$ or $2^\alpha - 1$. If p and q divide $2^\alpha + 1$, then $j = 1$. If neither of p, q divides $2^\alpha + 1$, then both p and q divide $2^\alpha - 1$ and so $j = 1$. When only one among p, q divides $2^\alpha + 1$, the other one divides $2^\alpha - 1$, implying $j = 2$. □

Theorem 4.2. *Let ρ be an odd prime. If p and q are distinct odd primes with pq dividing $\delta(\rho - 1)$ or $\delta(\rho + 1)$, then $U(\frac{(p-1)(q-1)}{2})$ is either equal to or an integral multiple of $U(\frac{p-1}{2})$. $U(\frac{q-1}{2})$.*

Proof. We have $\pi(\frac{pq-1}{2}) = \pi(\frac{(p-1)(q-1)}{2}) + \pi(\frac{p-1}{2}) + \pi(\frac{q-1}{2})$. First consider the case when both p and q are split-associated. In this case, $\pi(\frac{p-1}{2}) = \underbrace{(n + \cdots + n)}_{(s \text{ times})}$ where $sn = \frac{p-1}{2}$ and $s > 1$ and $\pi(\frac{q-1}{2}) = \underbrace{(m + \cdots + m)}_{(r \text{ times})}$ where $rm = \frac{q-1}{2}$ and $r > 1$. We have $\pi(\frac{(p-1)(q-1)}{2}) = \pi(2mnrs)$. By Theorem 4.1, $T\left(\frac{pq-1}{2}\right) = j \operatorname{lcm}(n, m), \ j \in \{1, 2\}$. Let us take $2\omega + 1 = pq$. Consider the satellite polynomial $\frac{H_\omega(x)}{H_{ns}(x) \ \times \ H_{mr}(x)}$ of $H_\omega(x)$. It attains all its roots in $\mathbb{F}_\rho$. The number of elements of $\mathbb{F}_\rho$ occurring as the roots of this polynomial is $2mnrs$. Since $T\left(\frac{pq-1}{2}\right) < 2mnrs$, these roots form more than one M-cycle. Consequently, by [14, Theorem 3.2], these roots split into local satellite polynomials of equal degree. Hence, the number of M-cycles formed by them is $\frac{2rs \gcd(n,m)}{j}, \ j \in \{1, 2\}$. Thus $U(\frac{(p-1)(q-1)}{2})$ is an integral multiple of $U(\frac{p-1}{2}).U(\frac{q-1}{2})$. A similar proof applies if exactly one or none of $p, \ q$ is split-associated. □

Corollary 4.1. *If $2\omega + 1 = p^2$ where p is an odd prime, then $U(\frac{p\ (p-1)}{2})$ is an integral multiple of $U(\frac{p-1}{2})$.*

Corollary 4.2. *The number of M-cycles in any part of $\pi(\omega)$ is a divisor of $U(\omega)$.*

From Theorems 3.1, 3.3 and Corollary 4.2, we deduce the following result.

Theorem 4.3. *Given $2\omega + 1 \in N$ and any background prime ρ of $2\omega + 1$, the roots of the polynomial $H_\omega(x)$ in $\mathbb{F}_\rho$ split into a certain number of polynomials $\in \{H_k(x)\}$ or satellite polynomials (universal or local) such that*

1. *the degree of the leading constituent polynomial of $H_\omega(x)$ with respect to $\mathbb{F}_\rho$ is divisible by the degree of any constituent polynomial of $H_\omega(x)$ and*
2. *the number of M-cycles in the largest part of $\pi(\omega)$ is divisible by the number of M-cycles in any part of $\pi(\omega)$.*

5 Invariants of a natural number

A condition for the polynomial $H_\omega(x)$ to attain roots in two different fields was established in [14, Theorem 5.6]. Now we take up the question of partitions in two such different fields. We have the following result.

Theorem 5.1 (Invariance of the partition under a change of background prime)**.** *The partitions of ω obtained with respect to any two distinct background primes for $2\omega + 1$ are the same.*

Proof. Case (i): Let $2\omega+1$ be a given non-split-associated prime. Let ρ and ρ' be two background primes for $2\omega + 1$. Suppose

$$\pi(\omega) = \begin{cases} (n) & \text{w.r.t } \rho \text{ and} \\ (n') & \text{w.r.t } \rho'. \end{cases} .$$

By [13, Theorem 6.1], there exist two M-cycles, one each in $\mathbb{F}_\rho$ and $\mathbb{F}_{\rho'}$ of lengths n and n' respectively such that the corresponding $\psi_{t,k}$-sequences attain zeros at ω in the respective finite fields. Therefore $2\omega + 1 \mid 2^n - 1$ and $2\omega + 1 \mid 2^{n'} - 1$ or $2\omega + 1 \mid 2^n + 1$ and $2\omega + 1 \mid 2^{n'} + 1$. Since the divisibility by $2\omega + 1$ is associated with the smallest n occurring as a power in $2^n - 1$ or $2^n + 1$, it follows that $n = n'$. This implies that $\pi(\omega)$ remains invariant under a change of the background prime for $2\omega + 1$.

Case (ii): Next suppose that $2\omega + 1$ is a split-associated prime. Suppose

$$\pi(\omega) = \begin{cases} (n_{1,1} + \cdots + n_{1,s_1}) & \text{w.r.t } \rho \text{ and} \\ (n'_{1,1} + \cdots + n'_{1,t_1}) & \text{w.r.t } \rho' \end{cases}$$

with $n_{1,1} = \cdots = n_{1,s_1}$ and $n'_{1,1} = \cdots = n'_{1,t_1}$. Again by [13, Theorem 6.1], there exist $s_1 > 1$ number of M-cycles in $\mathbb{F}_\rho$, each of length $n_{1,1}$ such that the corresponding $\psi_{t,k}$-sequences attain zeros at ω and a similar situation holds in $\mathbb{F}_{\rho'}$. Therefore we have $2\omega + 1 \mid 2^{n_{1,1}} - 1$ and $2\omega + 1 \mid 2^{n'_{1,1}} - 1$ or $2\omega + 1 \mid 2^{n_{1,1}} + 1$ and $2\omega + 1 \mid 2^{n'_{1,1}} + 1$. This implies that $n_{1,1} = n'_{1,1}$. Since $s_1 = \frac{\omega}{n_{1,1}}$ and $t_1 = \frac{\omega}{n'_{1,1}}$, it follows that $s_1 = t_1$.

Case (iii): Next suppose that $2\omega + 1$ is a composite number. Following the line of argument in cases (i) and (ii), we assert that $\mathrm{T}(\omega)$ is unaltered by a change of the background prime for $2\omega+1$. This implies that the number of elements in the largest part of $\pi(\omega)$ remains invariant under a change of the background prime for $2\omega + 1$. Now suppose that $2j + 1 \mid 2\omega + 1$. If $2j + 1$ is a prime, we can determine $\pi(j)$ by referring to case (i) or (ii). If $2j + 1$ is composite, we have to consider the divisors of $2j + 1$ and continue the procedure. The proof follows by induction. □

Definition 5.1 (Invariants of a natural number)**.** *The numbers* $n_{1,1},\ldots,n_{1,s_1}$*,* $n_{2,1},\ldots,n_{2,s_2}$*,* $n_{r,1},\ldots,n_{r,s_r}$*,* $\eta_1,\eta_2,\ldots,\eta_t, s_1,s_2,\ldots,s_r$ *in* (3.4) *are called the invariants of* $2\omega+1$ *with respect to the polynomial sequences* $\{F_k(x)\}$*,* $\{G_k(x)\}$ *and* $\{H_k(x)\}$*.*

By Corollaries 3.1 and 4.2, the $n's$ and $\eta's$, $n_{1,1}$ and each s_i in (3.4) divides s_1 for $i=2,\ldots,r$. From Theorem 3.3, it is seen that the degree of any polynomial in the standard polynomial factorization of $H_\omega(x)$ depends on the degree of $H_\omega(x)$ only and not on the particular field $\mathbb{F}_\rho$ where ρ is a background prime for $2\omega+1$. From Theorem 5.1, we deduce the following result.

Theorem 5.2. *The degrees of the* $H(x)$*-polynomials and the satellite polynomials in the standard polynomial factorization of* $H_\omega(x)$ *remain invariant whatever background prime* ρ *for* $2\omega+1$ *may be considered for the attainment of the roots of* $H_\omega(x)$ *in* $\mathbb{F}_\rho$*. Equivalently, the lengths of the* M*-cycles into which the roots of* $H_\omega(x)$ *in* $\mathbb{F}_\rho$ *decompose remain invariant whatever background prime* ρ *for* $2\omega+1$ *may be considered.*

Example 5.1. In this example we illustrate Theorem 5.1. Consider $\omega=66$. We see that 797 is a background prime for $2\omega+1$. The field $\mathbb{F}_{797}$ has the following M-cycles:

(I) $100\to434\to262\to100\to\cdots$

(II) $7\to47\to613\to380\to141\to751\to520\to215\to794\to7\to\cdots$

(III) $4\to14\to194\to175\to337\to393\to626\to547\to332\to236\to701\to447\to557\to214\to365\to124\to231\to757\to4\to\cdots$

(IV) $9\to79\to660\to436\to408\to686\to364\to192\to200\to148\to383\to39\to722\to44\to340\to33\to290\to413\to9\to\cdots$

(V) $34\to357\to724\to545\to539\to411\to752\to429\to729\to637\to94\to67\to502\to150\to182\to445\to367\to791\to34\to\cdots$

For the M-cycles (I) through (V), we have (n, ω) = (3, 3), (9, 9), (18, 66), (18, 66) and (18, 66). The 66 elements in these cycles are the roots of $H_{66}(x)$ *in* $\mathbb{F}_{797.}$ The partition of 66 with respect to $\mathbb{F}_{797}$ is got as

$$\pi(66)=(18+18+18)+(9)+(3).$$

This implies that the roots of $H_\omega(x)$ in $\mathbb{F}_{797}$ constitute the roots of $H_3(x)$, $H_9(x)$ and 3 local satellite polynomials of degree 18 each of $H_{66}(x)$.

Next we consider the background prime 1063 for $2\omega+1$. The following M-cycles exist in $\mathbb{F}_{1063}$:

(I) $510\to726\to889\to510\to\cdots$

(II) $42\to699\to682\to591\to615\to858\to566\to391\to870\to42\to\cdots$

(III) $81\to181\to869\to429\to140\to464\to568\to533\to266\to596\to172\to881\to169\to921\to1028\to160\to86\to1016\to81\to\cdots$

(IV) $103\to1040\to527\to284\to929\to946\to931\to414\to251\to282\to860\to813\to844\to124\to492\to761\to847\to945\to103\to\cdots$

(V) $192\to720\to717\to658\to321\to991\to930\to679\to760\to389\to373\to937\to992\to787\to701\to293\to807\to691\to192\to\cdots$

For the M-cycles (I) through (V), we have $(n, \omega) = (3, 3), (9, 9), (18, 66), (18, 66)$ and $(18, 66)$.

The elements in these cycles constitute the roots of $H_{66}(x)\ in\ \mathbb{F}_{1063}$. The partition of 66 with respect to $\mathbb{F}_{1063}$ is got as

$$\pi(66) = (18 + 18 + 18) + (9) + (3).$$

This indicates that the roots of $H_\omega(x)$ in $\mathbb{F}_{1063}$ constitute the roots of $H_3(x)$, $H_9(x)$ and 3 local satellite polynomials of degree 18 each of $H_{66}(x)$.

Thus we see that $\pi(66)$ is the same with respect to $\mathbb{F}_{797}$, as well as $\mathbb{F}_{1063}$.

6 Procedure for obtaining partitions

The phenomenon of invariance offers a procedure for the evaluation of the partition of a natural number in relation to H-sequence with respect to the concerned background prime. Consider the case when $2\omega + 1 = p_1 p_2$ where p_1 and p_2 are distinct primes. Let ρ_1 and ρ_2 be background primes for p_1 and p_2, respectively. Determine $\pi(\frac{p_1-1}{2})$ and $\pi(\frac{p_2-1}{2})$ with respect to $\mathbb{F}_{\rho_1}$ and $\mathbb{F}_{\rho_2}$, respectively. Let ρ be a background prime for $2\omega + 1$. One can directly evaluate $\pi(\frac{p_1-1}{2})$ and $\pi(\frac{p_2-1}{2})$ with respect to $\mathbb{F}_\rho$. However by Theorem 5.1, $\pi(\frac{p_1}{2})$ with respect to $\mathbb{F}_{\rho_1}$ and $\mathbb{F}_\rho$ are equal and similarly for $\pi(\frac{p_2-1}{2})$ with respect to $\mathbb{F}_{\rho_2}$ and $\mathbb{F}_\rho$. Consequently, it is enough if $\pi(\frac{(p_1-1)(p_2-1)}{2})$ is evaluated with respect to $\mathbb{F}_\rho$. Then one obtains $\pi(\omega)$ using the relation (3.2). A similar procedure applies if $2\omega + 1 = p^2$ where p is a prime.

7 Examples of partitions

To illustrate the procedure specified in the preceding section, two examples are furnished below.

Example 7.1. Consider $\omega = 104$. We have $2\omega + 1 = 209$. A background prime is 419. The following M-cycles exist in $\mathbb{F}_{419}$:

(1) $50 \to 403 \to 254 \to 407 \to 142 \to 50 \to \cdots$

(2) $45 \to 347 \to 154 \to 250 \to 67 \to 297 \to 217 \to 159 \to 139 \to 45 \to \cdots$

(3) $3 \to 7 \to 47 \to 112 \to 391 \to 363 \to 201 \to 175 \to 36 \to 37 \to 110 \to 366 \to 293 \to 371 \to 207 \to 109 \to 147 \to 238 \to 77 \to 61 \to 367 \to 188 \to 146 \to 364 \to 90 \to 137 \to 331 \to 200 \to 193 \to 375 \to 258 \to 360 \to 127 \to 205 \to 123 \to 43 \to 171 \to 328 \to 318 \to 143 \to 335 \to 350 \to 150 \to 291 \to 41 \to 3 \to \cdots$

(4) $5 \to 23 \to 108 \to 349 \to 289 \to 138 \to 187 \to 190 \to 64 \to 323 \to 415 \to 14 \to 194 \to 343 \to 327 \to 82 \to 18 \to 322 \to 189 \to 104 \to 339 \to 113 \to 197 \to 259 \to 39 \to 262 \to 345 \to 27 \to 308 \to 168 \to 149 \to 411 \to 62 \to 71 \to 11 \to 119 \to 332 \to 25 \to 204 \to 133 \to 89 \to 377 \to 86 \to 271 \to 114 \to 5 \to \cdots$

For the above M-cycles, we have $(n,\ \omega) = (5, 5), (9, 9), (45, 104)$ and $(45, 104)$, respectively. Therefore the partition for 104 is obtained as

$$\pi(104) = (45 + 45) + (9) + (5).$$

It is seen that 11 and 19 are divisors of 209 which in turn is a divisor of $2^{45} + 1$.

Example 7.2. Consider the background prime $\rho = 677$. The field $\mathbb{F}_{677}$ contains the following M-cycles:

(I) $124 \to 480 \to 218 \to 132 \to 497 \to 579 \to 124 \to \cdots$

(II) $8 \to 62 \to 457 \to 331 \to 562 \to 360 \to 291 \to 54 \to 206 \to 460 \to 374 \to 412 \to 492 \to 373 \to 342 \to 518 \to 230 \to 92 \to 338 \to 506 \to 128 \to 134 \to 352 \to 11 \to 119 \to 619 \to 654 \to 527 \to 157 \to 275 \to 476 \to 456 \to 95 \to 222 \to 538 \to 363 \to 429 \to 572 \to 191 \to 598 \to 146 \to 327 \to 638 \to 165 \to 143 \to 137 \to 488 \to 515 \to 516 \to 193 \to 12 \to 142 \to 529 \to 238 \to 451 \to 299 \to 35 \to 546 \to 234 \to 594 \to 117 \to 147 \to 620 \to 539 \to 86 \to 624 \to 99 \to 321 \to 135 \to 621 \to 426 \to 38 \to 88 \to 295 \to 367 \to 641 \to 617 \to 213 \to 8 \to \cdots$

For the above M-cycles, we have respectively $n = \omega = 6$ and $n = 78$, $\omega = 84$. The elements in the two M-cycles are the roots of $H_6(x)$ and $H_{84}(x)$ in $\mathbb{F}_{677}$. Consequently, we obtain the partition

$$\pi(84) = (78) + (6).$$

This relation yields the factor 13^2 of $2^{78} + 1$.

8 Partitions of prime factors of Mersenne numbers with prime exponents and Fermat numbers

The principle of partitions of natural numbers leads us to the following result.

Theorem 8.1 (Partitions of prime factors of Mersenne numbers with prime exponents and Fermat numbers)**.** *The following properties hold:*

1. *If $2\omega + 1$ is a prime factor of $2^q - 1$ with q a prime, then $\pi(\omega) = (q)$ or $\underbrace{(q + \cdots + q)}_{(s \text{ times})}$ with $s \in N$ and $s > 1$.*
2. *If $2\omega + 1$ is a prime factor of F_m $(m \geq 2)$, then $\pi(\omega) = \underbrace{(2^m + \cdots + 2^m)}_{(s \text{ times})}$ with $s \in N$ and $s > 1$.*

Proof. Let q be a prime. Then $2^q - 1$ is either a prime or composite. Consider the case when $2^q - 1$ is composite. Let $2\omega + 1$ be a prime factor of $2^q - 1$. By Corollary 3.1, $T(\omega) \mid q$. Since q is a prime, it follows that q occurs as an element of $\pi(\omega)$. If $2\omega + 1$ is a non-split-associated prime, then $\pi(\omega) = (q)$. In case $2\omega + 1$ is a split-associated prime we have $\pi(\omega) = \underbrace{(q + \cdots + q)}_{(s \text{ times})}$ with $s \in N$ and $s > 1$. Next consider the Fermat numbers $F_m = 2^{2^m} + 1$. These numbers have the property

$$F_m = F_0 F_1 \cdots F_{m-1} + 2.$$

From this relation, it follows that any two distinct Fermat numbers are relatively prime. Hence any Fermat number is either a prime or has a prime factor which does not divide any other Fermat number. Let $2\omega + 1$ be a prime factor of F_m $(m \geq 2)$. For the cases $2\omega + 1 = 17$ and 257, the partitions of ω are respectively given by $\pi(8) = (2^2 + 2^2)$ and $\pi(128) = \underbrace{(2^3 + \cdots + 2^3)}_{\text{(16 times)}}$. Let $2\omega + 1$ be a prime factor of F_m $(m \geq 2)$. The relation $T(\omega) \mid 2^m$ implies that 2^m occurs as an element of $\pi(\omega)$. The partition has to be of sharing type and the elements of the partition have to be equal. Consequently, we have $\pi(\omega) = \underbrace{(2^m + \cdots + 2^m)}_{(s \text{ times})}$ for some $s \in N$ and $s > 1$. □

9 Characterization of Mersenne primes

Certain results on harmonic numbers have been furnished by Cohen and Sorly [7]. These results have been employed by Brent, Crandall, Dilcher and van Halewyn [2] in the determination of the factors of Fermat numbers. One may refer to Bressoud [3], Brillhart and Johnson [5], Brillhart [4], Brillhart, Tonascia and Weinberger [6], Gostin [8], Kang [10], Karst [11] and Ribenboim [15] for several results on the factors of Mersenne and Fermat numbers.

Mersenne numbers are associated with even perfect numbers. Our objective is to establish the algebraic principle behind the factorization of Mersenne and Fermat numbers. This is accomplished by means of the theory of partitions developed in our study. We apply the results contained in the previous sections to understand the nature of even perfect numbers. We will consider the role played by the roots of $H(x)$-polynomials in the phenomenon of even perfect numbers.

It is well known (see for e.g., Hardy and Wright [9]) that a necessary condition for the primality of the Mersenne number $2^q - 1$ is that q be a prime. However, this condition is not sufficient. A question arises: When q is a prime, what makes $2^q - 1$ a prime and what makes it a composite? In the sequel we establish a sufficient condition for the primality of $2^q - 1$ when q is an odd prime. To illustrate the principle involved, one may consider the two particular cases $2^7 - 1$ and $2^{11} - 1$. The following questions arise: Why is that $2^7 - 1$ is a prime number? What is the reason for $2^{11} - 1$ being a composite number? The answers are obtained below.

Theorem 9.1. *Let q be an odd prime such that the Mersenne number $2^q - 1$ is composite. Then $\pi(2^{q-1} - 1)$ is of the form*

$$(q + \cdots + q) + (q + \cdots + q) + \cdots + (q + \cdots + q) + (q) \tag{9.1}$$

or

$$(q + \cdots + q) + (q + \cdots + q) + \cdots + (q + \cdots + q). \tag{9.2}$$

Proof. Let us take $2\omega + 1 = 2^q - 1$ so that $\omega = 2^{q-1} - 1$. Since $2^q - 1$ is composite, $\pi(\omega)$ has at least two parts with respect to any background prime ρ of $2\omega + 1$. As $2\omega + 1 \mid 2^q - 1$, it follows that $T(\omega)$ is q. Therefore the leading part of $\pi(\omega)$ is of the form $(q + \cdots + q)$. By Theorem 3.3, every element in $\pi(\omega)$ is a divisor of $T(\omega)$. Since q is a prime, every element in $\pi(\omega)$ has to be q only. Consequently, any part of $\pi(\omega)$ other than the leading part is of the form (q) or $(q + \cdots + q)$. Hence the theorem. □

From Theorem 9.1 we are able to deduce the following result of Fermat.

Theorem 9.2. *If q is an odd prime such that $2^q - 1$ is composite, then every prime factor p of $2^q - 1$ is of the form $2\lambda q + 1$ for some $\lambda \in N$.*

Theorem 9.3 (Test of primality of a Mersenne number)**.** *Let q be an odd prime. Then $2^q - 1$ is a prime if and only if $\pi(2^{q-1} - 1) = \underbrace{(q + \cdots + q)}_{(s\ times)}$ where $sq = 2^{q-1} - 1$ and $s > 1$.*

Proof. When q is a prime, by Fermat's theorem, $\frac{2^{q-1}-1}{q}$ is an integer. Let us take $2\omega + 1 = 2^q - 1$. If $2^q - 1$ is a prime, then $\pi(\omega)$ has only one part and consequently $\pi(2^{q-1} - 1)$ has the stated form. For the converse, we observe that whenever $2^q - 1$ is composite, there exists a part of $\pi(\omega)$ with the form (q) or $\underbrace{(q + \cdots + q)}_{(r \text{ times})}$ where $r \in N$ and $r < U(\omega)$. □

From Theorems 9.1 and 9.3 we are led to the following result.

Theorem 9.4 (Algebraic principle of Mersenne primes and Mersenne numbers with prime exponents)**.** *Let q be an odd prime and ρ a background prime for $2^q - 1$. The following properties hold.*

(i) $2^q - 1$ *is a prime if and only if all the constituent polynomials of $H_{(2^{q-1}-1)}(x)$ in $\mathbb{F}_\rho$ are of equal degree q and the zeros of all the $\psi_{t,k}$-sequences corresponding to the M-cycles occur at the same pivotal position in all the associated first components.*

(ii) $2^q - 1$ *is composite if and only if all the constituent polynomials of $H_{(2^{q-1}-1)}(x)$ in $\mathbb{F}_\rho$ are of equal degree q and at least two M-cycles formed by the roots of these polynomials have different ω values in the corresponding $\psi_{t,k}$-sequences.*

Example 9.1. The nature of the number $2^7 - 1$.
We consider the nature of the number $2^7 - 1$ from the theory of partitions. For $2^7 - 1$, a background prime is 509. The following M-cycles in the field $\mathbb{F}_{509}$ are of length 7 each:

(1) $3 \to 7 \to 47 \to 171 \to 226 \to 174 \to 243 \to 3 \to \cdots$

(2) $18 \to 322 \to 355 \to 300 \to 414 \to 370 \to 486 \to 18 \to \cdots$

(3) $19 \to 359 \to 102 \to 222 \to 418 \to 135 \to 408 \to 19 \to \cdots$

(4) $22 \to 482 \to 218 \to 185 \to 120 \to 146 \to 445 \to 22 \to \cdots$

(5) $41 \to 152 \to 197 \to 123 \to 366 \to 87 \to 441 \to 41 \to \cdots$

(6) $66 \to 282 \to 118 \to 179 \to 481 \to 273 \to 213 \to 66 \to \cdots$

(7) $83 \to 270 \to 111 \to 103 \to 427 \to 105 \to 334 \to 83 \to \cdots$

(8) $94 \to 181 \to 183 \to 402 \to 249 \to 410 \to 128 \to 94 \to \cdots$

(9) $104 \to 125 \to 353 \to 411 \to 440 \to 178 \to 124 \to 104 \to \cdots$

Corresponding to all these M-cycles, each one of the ψ-sequences attains the value of zero at $\omega = 63$. Since each one of the M-cycles is of length 7, each one of them contributes 7 roots of the polynomial $H_{63}(x)$ in the field $\mathbb{F}_{509}$. There are 9 such cycles. The elements of all the M-cycles together constitute the full complement of the roots of the polynomial $H_{63}(x)$ in the field $\mathbb{F}_{509}$. The partition of 63 is therefore obtained as

$$\pi(63) = \underbrace{(7 + \cdots + 7)}_{\text{(9 times)}}.$$

The elements of this partition are of sharing type with equal values of ω for the associated ψ-sequences, i.e., the ψ-sequences have the same pivotal position in the associated first components of the matrices $\mathfrak{a}(x)$. We have $2\omega + 1 = 127$. By [13, Theorem 8.2], it follows that 127 divides $2^7 - 1$ or $2^7 + 1$. It is checked that $2^7 - 1 = 127$. The fact that the ψ-sequences have the same pivotal position implies that $2^7 - 1$ is a prime. Thus we have obtained the algebraic principle explaining the primality of the Mersenne number $2^7 - 1$.

Example 9.2. The factorization of $2^{11} - 1$.
Consider the background prime $\rho = 4093$. There exist ninety three M-cycles in the field $\mathbb{F}_\rho$ of length 11 each. Among them, there is a unique M-cycle, viz.
$888 \to 2686 \to 2728 \to 908 \to 1769 \to 2307 \to 1347 \to 1208 \to 2154 \to 2345 \to 2124 \to 888 \to \cdots$ for which the ψ sequences attain the value of zero at $\omega = 11$. So this M-cycle contributes 11 roots of the polynomial $H_{1023}(x)$.
Corresponding to each one of the following four M-cycles
$25 \to 623 \to 3385 \to 1916 \to 3726 \to 3711 \to 2667 \to 3346 \to 1359 \to 936 \to 192 \to 25 \to \cdots,$
$73 \to 1234 \to 158 \to 404 \to 3587 \to 2268 \to 3014 \to 1827 \to 2132 \to 2192 \to 3773 \to 73 \to \cdots,$
$337 \to 3056 \to 3001 \to 1399 \to 745 \to 2468 \to 638 \to 1835 \to 2777 \to 515 \to 3271 \to 337 \to \cdots,$
$364 \to 1518 \to 4056 \to 1367 \to 2279 \to 3915 \to 3031 \to 2267 \to 2572 \to 894 \to 1099 \to 364 \to \cdots,$
the ψ-sequences attain the value of zero at $\omega = 44$. Each one of these M-cycles contributes 11 roots of the polynomial $H_{1023}(x)$. Thus they contribute $4 \times 11 = 44$ roots.

In the case of each one of the remaining eighty eight M-cycles, the ψ-sequences attain the value of zero at $\omega = 1023$. Each one of these M-cycles contributes 11 roots of the polynomial $H_{1023}(x)$. Thus they contribute $88 \times 11 = 968$ roots.

Hence, the total number of roots of the polynomial $H_{1023}(x)$ contributed by the above ninety three M-cycles is $11 + 44 + 968 = 1023$. Therefore the elements of all the ninety three M-cycles put together constitute the full complement of the roots of the polynomial $H_{1023}(x)$ in the field $\mathbb{F}_\rho$. The partition of 1023 with respect to the $H(x)$-sequence is thus obtained as

$$\pi(1023) = \underbrace{(11 + \cdots + 11)}_{\text{(88 times)}} + \underbrace{(11 + \cdots + 11)}_{\text{(4 times)}} + (11).$$

Hence, the elements of the partition are of sharing type with unequal values of ω for the associated ψ-sequences, i.e., the ψ-sequences have different pivotal positions in the associated first components of the matrices $\mathfrak{a}(x)$. It follows that each one of the numbers $2 \times 11 + 1$ and $8 \times 11 + 1$ divides $2^{11} - 1$ or $2^{11} + 1$. It is checked that 23 and 89 divide $2^{11} - 1$. Thus we obtain the factorization $2^{11} - 1 = 23 \times 89$.

That the ψ-sequences have different pivotal positions in the associated first components of the matrices $\mathfrak{a}(x)$ brings out the reason for the composite nature of the Mersenne number $2^{11} - 1$.

10 Characterization of Fermat primes

Theorem 10.1. *Suppose $m \geq 5 \in N$ with $2^{2^m} + 1$ composite. Then $\pi(2^{2^m - 1})$ is of the form $(2^m + \cdots + 2^m) + (2^m + \cdots + 2^m) + \cdots + (2^m + \cdots + 2^m)$.*

From Theorem 10.1 we are able to deduce the following result of Euler.

Theorem 10.2. *If $2^{2^m} + 1$ is composite, then each prime factor of $2^{2^m} + 1$ is of the form $2^{m+1}\lambda + 1$ for some $\lambda \in N$.*

Theorem 10.3 (Test of primality of a Fermat number)**.** $2^{2^m} + 1$ *is a prime if and only if*

$$\pi(2^{2^m - 1}) = \underbrace{(2^m + \cdots + 2^m)}_{(s \text{ times})},$$

where $s = 2^{2^m - m - 1}$.

Proof. If $2^{2^m} + 1$ is a prime, then $\pi(2^{2^m - 1})$ has only one part and consequently $\pi(2^{2^m - 1})$ has the stated form. If $2^{2^m} + 1$ is composite, then there is a part of $\pi(2^{2^m - 1})$ with the form $\underbrace{(2^m + \cdots + 2^m)}_{(r \text{ times})}$ where $r \in N$ and $r < U(2^{2^m - 1})$. □

Theorem 10.4 (Algebraic principle of Fermat primes and Fermat numbers)**.** *Let ρ be a background prime for $2^{2^m} + 1$. The following properties hold.*

(i) $2^{2^m} + 1$ *is a prime if and only if all the constituent polynomials of $H_{(2^{2^m} - 1)}(x)$ in $\mathbb{F}_\rho$ are of equal degree 2^m and the zeros of all the $\psi_{t,k}$-sequences corresponding to the M-cycles occur at the same pivotal position in all the associated first components.*

(ii) $2^{2^m} + 1$ *is composite if and only if all the constituent polynomials of $H_{(2^{2^m} - 1)}(x)$ in $\mathbb{F}_\rho$ are of equal degree 2^m and at least two M-cycles formed by the roots of these polynomials have different ω values in the corresponding $\psi_{t,k}$-sequences.*

Example 10.1 (Euler's result on the fifth Fermat's number)**.** Euler proved that the fifth Fermat's number is composite. We establish this result by means of the theory developed so far. Consider the field $\mathbb{F}_\rho$ with $\rho = 1283$. The following M-cycles in $\mathbb{F}_\rho$ are of length 32:

(1) $11 \to 119 \to 46 \to 831 \to 305 \to 647 \to 349 \to 1197 \to 979 \to 38 \to 159 \to 902 \to 180 \to 323 \to 404 \to 273 \to 113 \to 1220 \to 118 \to 1092 \to 555 \to 103 \to 343 \to 894 \to 1208 \to 491 \to 1158 \to 227 \to 207 \to 508 \to 179 \to 1247 \to 11 \to \cdots$

(2) $12 \to 142 \to 917 \to 522 \to 486 \to 122 \to 769 \to 1179 \to 550 \to 993 \to 703 \to 252 \to 635 \to 361 \to 736 \to 268 \to 1257 \to 674 \to 92 \to 764 \to 1212 \to 1190 \to 949 \to 1216 \to 638 \to 331 \to 504 \to 1263 \to 398 \to 593 \to 105 \to 759 \to 12 \to \cdots$

(3) $14 \to 194 \to 427 \to 141 \to 634 \to 375 \to 776 \to 447 \to 942 \to 809 \to 149 \to 388 \to 431 \to 1007 \to 477 \to 436 \to 210 \to 476 \to 766 \to 423 \to 590 \to 405 \to 1082 \to 626 \to 559 \to 710 \to 1162 \to 526 \to 829 \to 834 \to 168 \to 1279 \to 14 \to \cdots$

(4) $15 \to 223 \to 973 \to 1156 \to 731 \to 631 \to 429 \to 570 \to 299 \to 872 \to 846 \to 1083 \to 225 \to 586 \to 833 \to 1067 \to 466 \to 327 \to 438 \to 675 \to 158 \to 585 \to 945 \to 55 \to 457 \to 1001 \to 1259 \to 574 \to 1026 \to 614 \to 1075 \to 923 \to 15 \to \cdots$

(5) $27 \to 727 \to 1214 \to 910 \to 563 \to 66 \to 505 \to 989 \to 473 \to 485 \to 434 \to 1036 \to 706 \to 630 \to 451 \to 685 \to 928 \to 289 \to 124 \to 1261 \to 482 \to 99 \to 818 \to 679 \to 442 \to 346 \to 395 \to 780 \to 256 \to 101 \to 1218 \to 374 \to 27 \to \cdots$

(6) $29 \to 839 \to 835 \to 554 \to 277 \to 1030 \to 1140 \to 1202 \to 144 \to 206 \to 95 \to 42 \to 479 \to 1065 \to 51 \to 33 \to 1087 \to 1207 \to 642 \to 319 \to 402 \to 1227 \to 568 \to 589 \to 509 \to 1196 \to 1152 \to 480 \to 741 \to 1238 \to 740 \to 1040 \to 29 \to \cdots$

(7) $31 \to 959 \to 1051 \to 1219 \to 245 \to 1005 \to 302 \to 109 \to 332 \to 1167 \to 624 \to 625 \to 591 \to 303 \to 714 \to 443 \to 1231 \to 136 \to 532 \to 762 \to 726 \to 1044 \to 667 \to 969 \to 1086 \to 317 \to 413 \to 1211 \to 50 \to 1215 \to 773 \to 932 \to 31 \to \cdots$

(8) $35 \to 1223 \to 1032 \to 132 \to 743 \to 357 \to 430 \to 146 \to 786 \to 671 \to 1189 \to 1136 \to 1079 \to 558 \to 876 \to 140 \to 353 \to 156 \to 1240 \to 564 \to 1193 \to 400 \to 906 \to 997 \to 965 \to 1048 \to 54 \to 348 \to 500 \to 1096 \to 326 \to 1068 \to 35 \to \cdots$

(9) $37 \to 84 \to 639 \to 325 \to 417 \to 682 \to 676 \to 226 \to 1037 \to 213 \to 462 \to 464 \to 1033 \to 914 \to 161 \to 259 \to 363 \to 901 \to 943 \to 128 \to 986 \to 963 \to 1041 \to 827 \to 88 \to 44 \to 651 \to 409 \to 489 \to 481 \to 419 \to 1071 \to 37 \to \cdots$

(10) $107 \to 1183 \to 1017 \to 189 \to 1078 \to 967 \to 1063 \to 927 \to 1000 \to 541 \to 155 \to 929 \to 863 \to 627 \to 529 \to 145 \to 495 \to 1253 \to 898 \to 678 \to 368 \to 707 \to 760 \to 248 \to 1201 \to 307 \to 588 \to 615 \to 1021 \to 643 \to 321 \to 399 \to 107 \to \cdots$

Corresponding to all these M-cycles, each one of the ψ-sequences attains the value of zero at $\omega = 320$. Each one of the M-cycles contributes 32 roots of the polynomial $H_{320}(x)$. There are 10 such cycles. The elements of all the M-cycles together constitute the full complement of the roots of the polynomial $H_{320}(x)$ in the field $\mathbb{F}_\rho$. Consequently, the partition of 320 with respect to the $H(x)$-sequence is got as $\pi(320) = \underbrace{(32 + \cdots + 32)}_{\text{(10 times)}}$. Thus the elements of the partition are of sharing type with equal values of ω for the associated ψ-sequences, i.e., the ψ-sequences have the same pivotal position in the associated first compartments of the matrices $\mathfrak{a}(x)$. We have $2\omega+1=641$. So 641 divides $2^{32}-1$ or $2^{32}+1$. It is checked that 641 divides $2^{32}+1$. Thus we have obtained a proof for Euler's result on the composite nature of the Fermat's number F_5.

Next consider the background prime $\rho^{'}$ = 4398046512127. We have $\delta(\rho^{'}+1)=641\times 6700417$ where δ is the arithmetic function used to denote the odd part of a natural number [14, Definition 4.1]. One can check that

$$\pi(2147483648)=\underbrace{(32+\cdots+32)}_{(67004160 \text{ times})}+\underbrace{(32+\cdots+32)}_{(104694 \text{ times})}+\underbrace{(32+\cdots+32)}_{(10 \text{ times})}.$$

So the polynomial $\frac{H_{2147483648}(x)}{H_{3350208}(x)\,\times\,H_{320}(x)}$ splits into 67004160 local satellite polynomials of degree 32 each in $\mathbb{F}_{\rho'}$ while $H_{3350208}(x)$ and $H_{320}(x)$ split into 104694 and 10 local satellite polynomials, respectively, of degree 32 each. Thus one gets the factorization of F_5 as $2^{2^5}+1=641\times 6700417$. That the corresponding $\psi_{t,k}$-sequences have different pivotal positions in the associated first compartments of the matrices $\mathfrak{a}(x)$ is the reason why $2^{2^5}+1$ is rendered composite.

11 Algebraic principle of even perfect numbers

Now we consider the question: What makes a number perfect? We obtain the following answer. A natural number is said to be perfect if all its positive divisors, excluding itself, add up to itself. This is the traditional meaning of a perfect number. Euler proved that any even perfect number is of the form $2^{p-1}(2^p-1)$, where p is a prime (see for e.g., Hardy and Wright [9] and Roberts [16]).

11.1 Reasoning for the occurrence of even perfect numbers

'Being perfect' in the set of all natural numbers connotes a new meaning as has been brought out in our analysis. It is well known that an odd prime p gives rise to an even perfect number if and only if the Mersenne number 2^p-1 is a prime. The theory presented in this study throws a new light into an even perfect number. From Theorem 9.4, we are led to the following result.

Theorem 11.1 (Characterization of even perfect numbers)**.** *Let p be any given odd prime and ρ any background prime for 2^p-1. If all the $M(t)$-cycles constituting the roots of the polynomial $H_{(2^{p-1}-1)}(x)$ in $\mathbb{F}_\rho$ have the same pivotal position in all the associated first components in the matrices $\mathfrak{a}(M(t))$, then $2^{p-1}(2^p-1)$ is an even perfect number. If the zeros occur in different positions, then $2^{p-1}(2^p-1)$ is not perfect.*

From Theorem 11.1, Examples 9.1 and 9.2, it follows that $2^6(2^7-1)$ is an even perfect number while $2^{10}(2^{11}-1)$ is not perfect.

12 Conclusion

The method of cyclic sequences leads one to the concept of constituent polynomials of an $H(x)$-polynomial and the partition of a natural number. The fundamental theorem of partition of a given natural number with respect to the finite field $\mathbb{F}_\rho$ has been established. The partition of a natural number ω leads to a representation with respect to $\mathbb{F}_\rho$ of the splitting up of the polynomial $H_\omega(x)$ into a certain number of polynomials which are either in the $H(x)$-sequence or universal or local satellite polynomials of $H_\omega(x)$.

Given $2\omega + 1 \in N$ and any background prime ρ of $2\omega + 1$, we have proved that the roots of the polynomial $H_\omega(x)$ in $\mathbb{F}_\rho$ split into a certain number of polynomials $\in \{H_k(x)\}$ or satellite polynomials (universal or local) such that:

(1) the degree of the leading constituent polynomial of $H_\omega(x)$ with respect to $\mathbb{F}_\rho$ is divisible by the degree of any constituent polynomial of $H_\omega(x)$, and

(2) the number of M-cycles in the largest part of $\pi(\omega)$ is divisible by the number of M-cycles in any part of $\pi(\omega)$.

We have proved the following invariance property: The partitions of ω with respect to any two distinct background primes for $2\omega + 1$ are the same. We have deduced the following property: The degrees of the $H(x)$-polynomials and the satellite polynomials in the standard polynomial factorization of $H_\omega(x)$ remain invariant whatever background prime ρ of $2\omega+1$ may be considered for the attainment of the roots of $H_\omega(x)$ in $\mathbb{F}_\rho$. Equivalently, whatever background prime ρ for $2\omega + 1$ may be considered, the lengths of the M-cycles into which the roots of $H_\omega(x)$ in $\mathbb{F}_\rho$ decompose remain invariant.

The algebraic principle behind the factorization of Mersenne and Fermat numbers has been established. We have proved the following results:

(i) If $2\omega + 1$ is a prime factor of $2^q - 1$ with q a prime, then $\pi(\omega) = (q)$ or $\underbrace{(q + \cdots + q)}_{(s \text{ times})}$ with $s \in N$ and $s > 1$.

(ii) If $2\omega + 1$ is a prime factor of F_m $(m \geq 2)$, then $\pi(\omega) = \underbrace{(2^m + \cdots + 2^m)}_{(s \text{ times})}$ with $s \in N$ and $s > 1$.

If q is an odd prime and ρ is a background prime for $2^q - 1$, we have proved the following results:

(i) $2^q - 1$ is a prime if and only if all the constituent polynomials $H_{(2^{q-1}-1)}(x)$ in $\mathbb{F}_\rho$ are of equal degree q and the zeros of all the $\psi_{t,k}$-sequences corresponding to the M-cycles occur at the same pivotal position in all the associated first components.

(ii) $2^q - 1$ is composite if and only if all the constituent polynomials $H_{(2^{q-1}-1)}(x)$ in $\mathbb{F}_\rho$ are of equal degree q and at least two M-cycles formed by the roots of these polynomials have different ω values in the corresponding $\psi_{t,k}$-sequences.

When ρ is a background prime for $2^{2^m} + 1$, we have proved:

(i) $2^{2^m} + 1$ is a prime if and only if all the constituent polynomials of $H_{(2^{2^m-1})}(x)$ in $\mathbb{F}_\rho$ are of equal degree 2^m and the zeros of all the $\psi_{t,k}$-sequences corresponding to the M-cycles occur at the same pivotal position in all the associated first components.

(ii) $2^{2^m} + 1$ is composite if and only if all the constituent polynomials of $H_{(2^{2^m-1})}(x)$ in $\mathbb{F}_\rho$ are of equal degree 2^m and at least two M-cycles formed by the roots of these polynomials have different ω values in the corresponding $\psi_{t,k}$-sequences.

The theory in this study throws a new light into the phenomenon of even perfect numbers. Let p be any given odd prime and ρ any background prime for $2^p - 1$. Then $2^{p-1}(2^p - 1)$ is an even perfect number if all the roots of the polynomial $H_{(2^{p-1}-1)}(x)$ occur in the same position in the ψ-sequences. In case the zeros occur in different positions, $2^p - 1$ splits into a product of primes in $\mathbb{F}_\rho$ and we do not get a perfect number. Thus the method of cyclic sequences in a finite field provides an algebraic interpretation of the phenomenon of even perfect numbers.

Acknowledgements

The author is grateful to the reviewers for the suggestions to improve the presentation.

References

[1] Andrews, G. (1998). *The Theory of Partitions*. Cambridge University Press.

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

[3] Bressoud, D. M. (1989). *Factorization and Primality Testing*. Springer Verlag.

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

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

[6] Brillhart, J., Tonascia, J., & Weinberger, P. (1971). On the Fermat quotient. In: *Computers in Number Theory*, Academic Press.

[7] Cohen, G. L., & Sorli, R.M. (1998). Harmonic seeds. *The Fibonacci Quarterly*, 36(5), 386–390.

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

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

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

[11] Karst, E. (1961). New factors of Mersenne numbers. *Mathematics of Computation*, 15, 51–55.

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

[13] 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.

[14] Ramasamy, A. M. S. (2024). Sequences in Finite Fields yielding divisors of Mersenne, Fermat and Lehmer Numbers, II. *Notes on Number Theory and Discrete Mathematics*, 30(2), 236-252.

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

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