RFSC-04-02
Revised

A METHOD FOR GENERATING MERSENNE PRIMES AND THE EXTENT OF THE SEQUENCE OF THE EVEN PERFECT NUMBERS

Simon Davis

Research Foundation of Southern California
8837 Villa La Jolla Drive #13595
La Jolla, CA 92039

Abstract. A condition is obtained for the generation of new Mersenne primes from a combination of Mersenne numbers with prime indices. It is verified that all known Mersenne prime indices greater than 19 have the form $p_1 + p_2 - 1$, where $2^{p_1} - 1$ is prime and $2^{p_2} - 1$ is composite. Arithmetical sequences for the exponents of composite Mersenne numbers are obtained from partitions into consecutive integers, and congruence relations for products of two Mersenne numbers suggest the existence of infinitely many composite integers of the form $2^p - 1$ with p prime. The congruence properties of polynomial exponents are found also to be useful in a mechanism for generating new Mersenne primes and establishing the existence of infinitely many primes of this kind.

MSC:11N32, 11N80, 11P83

Keywords: *Mersenne primes, perfect numbers, composite Mersenne numbers, polynomial approximation*

1. Introduction

The perfect numbers, defined by a condition on the sum of the divisors, represented by a sequence of integers that has been conjectured to have connections with the ideal characteristics of physical systems. After a geometrical proof by Euclid that an integer of the form $2^{p-1}(2^p-1)$, with 2^p-1 being prime, would be perfect number [3], it was hypothesized later that all perfect numbers were even, every even perfect number equals $2^{p-1}(2^p-1)$ for some prime 2^p-1 and there are infinitely many perfect numbers [28]. The next perfect numbers were discovered in the early thirteenth century [30]. After a series of perfect numbers verified only until $p=19$ [2], a systematic investiagation of the perfect numbers began with the letter of Fermat to Mersenne [10] and the following theorems: 2^n-1 is composite if n is composite; if n is prime, 2^n-2 is a multiple of $2n$; if n is prime and p is a prime divisor of 2^n-1, then $p-1$ is a multiple of n [11]. Further primes of the kind 2^p-1 were suggested, and it was demonstrated by Euler $2^{30}(2^{30}-1)$ [8] was a perfect number and further the uniqueness of $2^{p-1}(2^p-1)$ for every even perfect number [9]. No new perfect numbers were found until $2^{60}(2^{61}-1)$ [31], whereas it had been shown that $2^{67}-1$ was not a prime [20] and $2^{127}-1$ was a Mersenne prime [21]. Lucas also proved that every perfect number greater than 6 must end in the digits 16, 28, 36, 56, 76 and 96 [22]. The last result led to the conjecture of Catalan that the sequence $\left(2^p-1, 2^{2^p-1}-1, ...\right)$. consists of primes for $p=2$ [1]. The infinite sequence of even perfect numbers then would follow from this conjecture and the infinite Catalan sequence. While $2^{88}(2^{89}-1)$ was verified as a perfect number in 1911 [32], the use of computers has been found to be necessary for the larger of the 51 known Mersenne primes and the extent of this sequence remained to be established.

Further properties of perfect numbers include the form of the prime index p being $1+T_n$, where T_n is a triangular number [6], the equality of x^3+1 and a perfect number only for the integer 28 [25], the integrality of the harmonic mean of the divisors [29] and the proportionality of the number of divisors of a perfect number N to $ln\ ln\ N$ [4].

The Lucas-Lehmer test, together with several characteristics of prime divisors of Mersenne numbers that are valid for all Lucas sequences, can be used to determine theoretically whether the integer 2^p-1 is prime. The congruence $s_{p-2} \equiv 0\ (mod\ 2^p-1)$, $s_n = s_{n-1}^2 - 2$ [19][21], is satisfied by the known Mersenne primes, although the difficulty of the computation increases for large values of n.

The conjecture of the existence of infinitely many Mersenne primes and the problem of establishing the infinite extent of the sequence of composite Mersenne numbers with prime indices [7][9][14][18][26][28][40] may be solved without consideration of specific values of the exponent. The generality of these statements allows for the proofs to be based on conditions imposed on integers of the same order as the exponents. It is shown in §2, for example, that all known Mersenne primes greater than $2^{19}-1$ are shown to have exponents

of the form p_1+p_2-1 where p_1 is a Mersenne prime index and p_2 is a composite Mersenne number index.

It was hypothesized by Euler and proven by Lagrange that 2^p-1 is a composite Mersenne number if the prime p has the form $4k+3$ and $2p+1$ is a prime. An infinite number of Sophie Germain primes congruent to 3 modulo 4 would imply the existence of an infinite number of composte Mersenne numbers with prime exponents. The Mersenne numbers also have a geometrical representation which may be used to derived congruence relations for compositeness based on the partition of the array representing 2^n-1. The solutions to the congruence relations yield arithmetical sequences for the exponent. However, the greatest commom denominator of the initial term and the difference can be equated to $ord_{2^m-k}(k)$ for some m, k, such that none of the integers in the sequence are prime. Nevertheless, this allows a characterization of the set of exponents greater than 6 of composite Mersenne numbers. The congrence relations for $2^{p_1+p_2-1}-1$ provide a further indication of the existence of infinitely many composite Mersenne numbers with prime exponents.

Given a set of Mersenne prime indices of the form $4k+3$, conditions on the next prime of this kind are given in §4. A proof of the existence of infinitely many Mersenne primes is given in §5. The existence of a finite number of prime solutions to $a^{f(n)}-b^{f(n)} \equiv 0\ (mod\ n)$ when $f(x)$ does not have a zero at $x=1$, is used to develop an algorithm for locating the next Mersenne prime based on the intersections of polynomials at prime arguments. The approximation of 2^y-1 by rational-coefficient polynomials is used to determine the asymptotic density of Mersenne primes, proving the infinite extent of the sequence of such primes.

2. The Exponents of Mersenne Numbers and Arithmetical Progressions

There are two infinite sequences, of Mersenne numbers of odd index, and primes, in the arithmetical progression $6n+1$, $n \in \mathbb{Z}^+$, and the coincidences of these two sequences determine whether the set of even perfect continues indefinitely.

Since $6n+1$ can be factorized only if n has the form $6xy \pm (x+y)$ with $x, y \in \mathbb{Z}^+$ [22], the Mersenne number 2^p-1 is prime only if it equals $6n+1$, $n=6xy \pm (x+y)+z$, $z \neq 0$, with $6xy \pm (x+y)+z \neq 6x'y' \pm (x'+y')$ for any integers x', y'. Given the condition $2^p-1=(6x \pm 1)(6y \pm 1)$, consider two primes p_1 and p_2 such that

$$\begin{aligned} 2^{p_1}-(6z_1+1) &= (6x_1 \pm 1)(6y_1 \pm 1) = 6h_1+1 \qquad & h_1 &= 6x_1y_1 \pm (x_1+y_1) \\ 2^{p_2}-(6z_2+1) &= (6x_2 \pm 1)(6y_2 \pm 1) = 6h_2+1 \qquad & h_2 &= 6x_2y_2 \pm (x_2+y_2) \end{aligned} \tag{2.1}$$

Multiplying these two integers gives

$$2^{p_1+p_2}-(6z_1+1)(6z_2+1)-(6z_1+1)(6h_2+1)-(6z_2+1)(6h_1+1) = (6h_1+1)(6h_2+1) \tag{2.2}$$

or equivalently

$$2^{p_1+p_2-1} = [3(h_1+z_1)+1][6(h_2+z_2)+2] \tag{2.3}$$

If $z_{/} = 0$, and $2^{p_1}-1$ is prime, while z_2 is set equal to zero, $2^{p_2}-1$ is allowed to be composite,

$$2^{p_1+p_2-1} - [6((1-\gamma_1)z_1+(1-\gamma_2)h_1+(1-\gamma_3)h_2)+1] = 6(3(h_1+z_1)h_2+\gamma_1 h_1+\gamma_2 z_1+\gamma_3 h_2)+1 \tag{2.4}$$

for some fractions $\gamma_1, \gamma_2, \gamma_3$ with $3(h_1+z_1)h_2+\gamma_1 h_1+\gamma_2 z_1+\gamma_3 h_2 = 6x'y' \pm (x'_+ y')$, $x', y' \in \mathbb{Z}$. The Mersenne number $2^{p_1+p_2-1}-1$ is prime if there is no solution to Eq.(2.4) with $\gamma_1 = \gamma_2 = \gamma_3 = 1$. If p_1 is a given Mersenne prime index, it can be conjectured that $p_1 - 1$ may be expressed as the difference between two primes p and p_2, since an even integer $2N$ equals $p - p_2$ if $2(N+p_2)$ is given by the sum of the two primes $p,\ p_2$.

The estimated number of prime pairs $(p, p+2N)$ with $p \leq x$ is conjectured to be

$$\pi_{2N}(x) \sim 2C_2 \frac{x}{(log\ x)^2} \prod_{\substack{p>2 \\ p|N}} \frac{p-1}{p-2} \tag{2.5}$$

where C_2 is the twin-prime constant $\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)$ [27][39], and

$$\pi_2(x) \leq 6.836 C_2 \frac{x}{(log\ x)^2}\left[1+\mathcal{O}\left(\frac{log\ log\ x}{log\ x}\right)\right] \tag{2.6}$$

Theorem. Every finite even positive integer $2N$ can be expressed as the difference between two primes if the Goldbach conjecture is valid.

Proof. For any even integer $2N$, $N > 2$, there exist two primes $q_1,\ q_2$ $2N = q_1 + q_2$ when the Goldbach conjecture [9] is correct. This equality implies a relation of the form $2\bar{N} = \bar{q}_1 - \bar{q}_2$, $\bar{q}_1,\ \bar{q}_2$ prime, for some $\bar{N} < N$, since $2(N-q_2) = q_1 - q_2$. It may be assumed that this property holds for all integers $1 \leq \tilde{N} \leq \bar{N}$ and that the lesser prime in each of the differences is bounded above by $2\tilde{N}-2$. The existence of a prime pair with a difference equal to an arbitrary even integer shall be demonstrated by induction on $\bar{N}$.

$$\begin{aligned} 2\bar{N}+2 &= \bar{q}_1 - \bar{q}_2 + 2 = 2N + 2 - 2\bar{q}_2 \\ &= q_3 + q_4 - 2\bar{q}_2 = (q_3 - \bar{q}_2 + k) - (\bar{q}_2 - q_4 + k) \end{aligned} \tag{2.7}$$

Since $q_3 + q_4 = \bar{q}_1 + \bar{q}_2 + 2$, the indices can be chosen such that $q_3 > \bar{q}_1$ and $q_4 < \bar{q}_2 + 2$ or $\bar{q}_1 > q_3 > \bar{q}_2$, $q_4 > \bar{q}_2 + 2$ unless $q_3 = \bar{q}_1$, $q_4 = \bar{q}_2 + 2$. If the equalities are valid, then $2\bar{N}-2 = q_3 - q_4$. Continuing this process with $2N+2$ replaced by $2N+2\iota$, $\iota \geq 2$, it follows that the equalities would imply that all even integers less than $2\bar{N}$ can be expressed as differences between pairs of primes even when arbitrarily large values of $\bar{N}$ are chosen by

subtracting $2q_6$ from an arbitrarily large integer $N' = q_5 + q_6$. Consequently, the equalities would imply that every even integer is equal to the difference between two primes.

Suppose then that the first set of inequalities holds. Then $q_3 - \bar{q}_2 - 1 > 0$ and $\bar{q}_2 - q_4 + 1 > 0$. Since

$$2\bar{N} + 2 = (q_3 - \bar{q}_2 + k + k') - (\bar{q}_2 - q_4 + k + k') \tag{2.8}$$

and $\bar{q}_2 - q_4 + k + k' = \bar{q}_2 + k_1 + k' - (q_4 - k_2)$, $k_1 + k_2 = k$, $k_1, k_2,\ k'$ can be chosen such that $q_4 - k_2 = \bar{q}_2 + k_1 + k' - \bar{p}_2$ with $\bar{q}_2 + k_1 + k'$ and $\bar{p}_2$ prime, since $q_4 + k_2 < 2\bar{N}$ and the difference between two primes fixes $k_1 + k'$. Then, k' can be adjusted to fix $q_3 - \bar{q}_2 + k + k'$ to be prime. It follows that $2\bar{N} + 2 = q_3 - \bar{q}_2 + k + k' - \bar{p}_2$ is a difference between two primes, with $\bar{p}_2 < 2\bar{N}$.

If $q_3 < \bar{q}_1$, $q_4 > \bar{q}_2 + 2$, consider the equality

$$2\bar{N} = \bar{q}_1 - \bar{q}_2 + 2 = (\bar{q}_1 + q_4 + k + k' + 2) - (q_4 - \bar{q}_2 + k + k') \tag{2.9}$$

As $q_4 - \bar{q}_2 + k + k' = (q_4 + k_1 + k') - (\bar{q}_2 - k_2)$ and $\bar{q}_2 - k_2$ is an even integer less than $2\bar{N}$, $\bar{q}_2 - k_2 = q_4 + k_1 + k' - \bar{p}_3$ where $\bar{p}_3$ is prime and $k_1 + k'$ is adjusted to render $q_4 + k_1 = k'$ to be prime. Then k' also can be chosen such that $\bar{q}_1 + q_4 + k + k' + 2$ is prime.

By induction, it follows that any even integer is the difference between two primes.

■

It follows that the conjecture for primes of the form $4k-1$, such that there would exist a prime $4k' + 1$ with the the difference $2 \cdot (4k'' + 1)$ being any given even number [12], is valid.

Since it can be established for any even number $2n$ that there are pairs of primes differing by $2n$, the pair (p, p_2) can be presumed to exist. Indeed, if $p - p_1$ is set equal to $p_2 - p_3$ for primes $p_2,\ p_3 \geq 3$, a relation of form Eq.(2.4) cannot be satisfied because division by additional powers of 2 yields a fractional term, and, if $p_1,\ p$ are odd primes, $p_3 \neq 2$. Therefore, p must have the form $p_1 + p_2 - 1$. This property can be verified for the following pairs of prime indices (p_1, p_2):

$(3, 11); (7, 11); (3, 29); (19, 43); (31, 59); (61, 47); (61, 67); (89, 433); (61, 547);$
$(607, 673); (607, 1597); (2203, 79); (2281, 937); (2281, 1973); (2203, 2221); (4253, 5447);$
$(4253, 6961); (2281, 17657); (89, 21613); (2281, 20929); (3217, 41281); (9941, 76303)$
$(607, 109897); (44497, 87553); (23209, 192883); (132049; 624791); (19937, 839497)$
$(132049, 1125739); (86243, 1312027); (86243, 2889979); (21701, 3049677);$
$(3071377, 3901217); (216091, 13250827); (110503; 20885509); (1257787, 22778797);$
$(110503, 25874449); (3217, 30399241); (3021377, 29561281)$

The prime pairs (p_1, p_2) with $2^{p_1} - 1$, $2^{p_2} - 1$ and $2^{p_1+p_2-1} - 1$ prime, $\{(2,2); (3,3); (3,5); (7,7); (5,13); (3,17); (7,13); (13,19); (31,31)\}$ complement the larger set when $p_1 + p_2 - 1 = 3, 5, 7, 13, 17, 19, 31, 61$.

One subset of the composite Mersenne numbers of the form $2^{p_1+p_2-1} - 1$ can be constructed from the integer solutions to the following sets of equations

$$\begin{aligned} h_1 &= 6x_1y_1 + (x_1 + y_1) \qquad h_2 = 6x_2y_2 + (x_2 + y_2) \\ w_1 + w_2 &= 3(x_1 + y_1 + z_1)(x_2 + y_2) + (x_1 + y_1 + z_1) + (x_2 + y_2) \\ w_1w_2 &= 18x_1y_1x_2y_2 + 3x_1y_1(x_2 + y_2) + 3x_2y_2(x_1 + y_1 + z_1) + (x_1y_1 + x_2y_2) \end{aligned} \tag{2.10}$$

$$\begin{aligned} h_1 &= 6x_1y_1 - (x_1 + y_1) \qquad h_2 = 6x_2y_2 + (x_2 + y_2) \\ w_1 + w_2 &= -3(x_1 + y_1 - z_1)(x_2 + y_2) + 6(x_1y_1 + x_2y_2) - (x_1 + y_1 - z_1) + (x_2 = y_2) \\ w_1w_2 &= 18x_1y_1x_2y_2 + 3x_1y - 1(x_2 + y - 2) - 3x_2y_2(x_1 + y_1 - z_1) + (x_1yy_1 + x_2y_2) \end{aligned} \tag{2.11}$$

$$\begin{aligned} h_1 &= 6x_1y_1 + (x_1 + y_1) \qquad h_2 = 6x_2y_2 - (x_2 + y_2) \\ w_1 + w_2 &= -3(x_1 + y_1 + z_1)(x_2 + y_2) + 6(x_1y_1 + x_2y_2) + (x_1 + y_1 + z_1) - (x_2 + y_2) \\ w_1w_2 &= 18x_1y_1x_2y_2 - 3x_1y_1(x_2 + y_2) + 3x_2y_2(x_1 + y_1 + z_1) + (x_1y_1 + x_2y_2) \end{aligned} \tag{2.12}$$

$$\begin{aligned} h_1 &= 6x_1y_1 - (x_1 + y_1) \qquad h_2 = 6x_2y_2 - 9x_2 + y_2) \\ w_1 + w_2 &= 3(x_1 + y_1 - z_1)(x_2 + y_2) - (x_1 + y_1 + z_1) - (x_2 + y_2) \\ w_1w_2 &= 18x_1y_1x_2y_2 - 3x_1y_1(x_2 + y_2) - 3x_2y_2(x_1 + y_1 - z_1) + (x_1y_1 + x_2y_2) \end{aligned} \tag{2.13}$$

Consider the equations determined by the equations $u + v = h_1 + z_1 + h_2$ and $uv = \frac{1}{2}(h - 1 + z_1)h_2$. These two conditions imply

$$2u^2 - 2(h_1 + z_1 + h_2)u + (h_1 + z_1)h_2 = 0 \tag{2.14}$$

and

$$u = \frac{1}{2}\left[h_1 + z_1 + h_2 \pm \sqrt{(h_1 + z_1 + h_2)^2 - 2(h - 1 + z_1)h_2}\right] \tag{2.15}$$

Then u is integer only if $(h - 1 + z_1)^2 + h_2^2$ is the square of an integer. Since Pythagorean triples are multiples of the triples $(3 + 2n, 4 + 6n + 2n^2, 5 + 6n + 2n^2)$, there is no solution for $h_1 + z_1$ and h_2 as both integers must be odd.

More generally,

$$\begin{aligned} u + v &= \kappa_1(h_1 + z_1)h_2 + \kappa_2(h_1 + z_1 + h_2) \\ uv &= \kappa_3(h_1 + z_1)h_2 + \kappa_4(h_1 + z_1 + h_2) \end{aligned} \tag{2.16}$$

with

$$\begin{aligned} \kappa_1 + 6\kappa_3 &= 3 \\ \kappa_2 + 6\kappa_4 &= 1 \\ \kappa_1, \kappa_2, \kappa_3, \kappa_4 &\in \mathbb{Q} \end{aligned} \tag{2.17}$$

Integrality of u and v requires that $\kappa_1(h_1+z_1)h_2+\kappa_2(h_1+z_1+h_2)$ and $\frac{3-\kappa_1}{6}(h_1+z_1)h_2+\frac{1-\kappa_1}{6}(h_1+z_1+h_2)$ are integer, while $[\kappa_1(h_1+z_1)h_2+\kappa_2(h_1+z_1+h_2)]^2-4\left[\frac{3-\kappa_1}{6}h_1+z_1)h_2+\frac{1-\kappa_1}{6}(h_1+z_1+h_2)\right]$ is the square of an integer.

Additional constraints can be placed on $h-1+z_1$, h_2 as the equality of $6[3(h_1+z_1)h_2+(h_1+z_1)+h_2]+1$ and $2^{p-1+p_2-1}-1$ would imply congruence conditions. First, after division by 2, it follows that either $h-1+z-1 \equiv 0 \ (mod\ 4)$, $h_2 \equiv 5 \ (mod\ 8)$; $h_1+z_1 \equiv 5 \ (mod\ 8)$, $h_2 \equiv 0 \ (mod\ 4)$; $h_1+z_1 \equiv 1 \ (mod\ 4)$, $h_2 \equiv 3 \ (mod\ 4)$; $h_1+z_1 \equiv 3 \ (mod\ 4)$, $h_2 \equiv 1 \ (mod\ 4)$. Since $3(h_1+z_1)h_2+(h_1+z_1)+h_2 \equiv \frac{2^n-1}{3} \ (mod\ 2^n)$, *n even* and $3(h-1+z_1)h_2+(h_1+z_1)+h_2 \equiv \frac{2^{n+1}-1}{3} \ (mod\ 2^n)$, *n odd*.

Based on the pairwise relations between Mersenne prime indices, a sum extended over a set of such integers can be derived. Since $p'_n = p_{kc}+p'_\ell-1$ for some composite Mersenne number index p_{kc} and $\ell < n$ and $p_{kc}-1$ may be expressed either as the sum of two even integers that are differences between a Mersenne prime index and a composite Mersenne index, or the sum of two primes by the Goldbach conjecture, the process can be iterated until all of the addends are either Mersenne prime indices, with either sign, or twice the previous index or ± 1.

The relations in Appendix A have a form similar to the equations for the sequence or primes [44][45]

$$\begin{aligned} p_{2n} &= 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-2} + p_{2n-1} \\ p_{2n+1} &= 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-1} + 2p_{2n}. \end{aligned} \tag{2.18}$$

The equations are also consistent with the estimate of the number of Mersenne primes with index p between x and $2x$ [16][47]. It is possible also to extend the sequence of Mersenne prime indices by forming combinations having the form in Eq.(2.18) and using any of the various test to verify that 2^p-1 is prime.

3. Congruence Relations for Mersenne Prime Indices of the Form $4k+3$

Let $p \equiv 3 \ (mod\ 4)$ be a Mersenne prime index [45] such that

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \equiv 0 \qquad (mod\ p) \tag{3.1}$$

or equivalently

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} = k_1 p \tag{3.2}$$

for some K_1. The congruence

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} \equiv 0 \pmod{p'} \tag{3.3}$$

for some prime $p' > p$ with $p' \equiv 3 \ (mod\ 4)$ is equivalent to

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} = \sum_{n=1}^{\bar{N}} K_{2n} p'^n \tag{3.4}$$

Since $\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}}$ is integer for odd p,

$$\begin{aligned} \sum_{n=1}^{\bar{N}} K_{2n} p'^n - K_1 p = \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} - \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \\ - \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \\ = f(p') \end{aligned} \tag{3.5}$$

Suppose for arbitrarily large x that the function

$$f(x) = \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{x+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} > 0 \tag{3.6}$$

can be approximated by a polynomial of degree N

$$a_N x^N + ... + a_1 x + a_0 \tag{3.7}$$

such that the polynomial takes the same values as $f(x)$ at $N+1$ integer points including prime values less than or equal to p'. The existence of a prime p' satisfying the congruence conditions determined by solutions to the equation

$$K_{2\bar{N}} p'^{\bar{N}} + ... + K_{21} p' = f(p') + k_1 p \tag{3.8}$$

Since $f(x)$ equals $a_N x^N + ... + a_1 x + a_0$ at $x = p'$, the congruence

$$a_0 + K_1 p \equiv 0 \pmod{p'} \tag{3.9}$$

is required. The constant term may be adjusted through the choice of the polynomial $a_N x^N + ... + a_1 x + a_0$ or equivalently the number of points of equality, $N+1$. As the Lagrangian interpolation polynomial is

$$\begin{aligned} L(x) &= \sum_{n=0}^{N} I_n(x) f(x_n) \\ I_n(x) &= \frac{P(x)}{(x-x_n)P'(x_n)} \\ P(x) &= \prod_{n=0}^{N} (x-x_n) \end{aligned} \tag{3.10}$$

For the function

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{x+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \tag{3.11}$$

the Lagrangian interpolation would be

$$\begin{aligned} L(x) = \sum_n \prod_{n\neq m} \frac{x-x_m}{x_n-x_m} \Bigg[&\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{x+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{x+1}{2}} \\ &- \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \Bigg] \end{aligned} \tag{3.12}$$

The congruence condition is now

$$\begin{aligned} \sum_n \prod_{n\neq m} \frac{x-x_m}{x_n-x_m} \Bigg[&\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{x+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{x+1}{2}} \\ &- \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \Bigg] + K_1 p \equiv 0 \pmod{p'} \end{aligned} \tag{3.13}$$

Given the congruence relation for p' to be a Mersenne prime index, Eq.(3.13) implies

$$\left[1 - \sum_n \prod_{n\neq m} \frac{(p'-x_m)}{(x_n-x_m)}\right] K_1 p \equiv 0 \pmod{p'} \tag{3.14}$$

when $\sum_n \frac{(p'-x_m)}{(x_n-x_m)} p$ is an integer. However, since $\{x_n\}$ should contain p' for consistency with the Mersenne prime index congruence condition for p', this relation leads to no further

constraints on p'. It shall be shown nevertheless that a set of interpolating polynomials may be used to determine the existence of successively larger Mersenne primes.

4. On a Polynomial Algorithm for Generating Mersenne Primes

The solutions to the equation $a^{f(n)} \equiv b^{f(n)}\ (mod\ n)$ for an integer-valued function $f(n)$ also must satisfy $a^{(n-1)g(n)+f(1)} - b^{(n-1)g(n)+f(1)} \equiv a^{f(1)} - b^{f(1)} \equiv 0\ (mod\ n)$, when n is prime, $gcd(a,n) = gcd(b,n) = 1$ and $g(n)$ is an integer defined by $f(n) = (n-1)g(n)+f(1)$. If $f(n)$ is a polynomial with integer coefficients, $f(n) = \sum_{k\geq 0} a_k n^k$, with $a_k = 0$ for k greater than a finite lower bound,

$$f(n) = f(1) + (n-1)\left(f'(1) + \frac{1}{2!}f''(1)(n-1) + \frac{1}{3!}f'''(1)(n-1)^2 + ...\right) \tag{4.1}$$

and $g(n)$ is integer since

$$\frac{1}{\ell!}f^{(\ell)}(1) = \sum_{k\geq 0}\frac{1}{\ell!}a_k(k+\ell)(k+\ell-1)...(k+1) \tag{4.2}$$

Given that $f(1)$ and $f(n)$ are integer, an integer $g(n)$ can be found such that $f(n) \equiv f(1) + (n-1)g(n)\ (mod\ n)$. Then

$$a^{f(n)} - b^{f(n)} \equiv a^{f(1)+(n-1)g(n)+Kn} - b^{f(1)+(n-1)g(n)+Kn} \equiv a^{f(1)+K} - b^{f(1)+K} \quad (mod\ n) \tag{4.3}$$

With an appropriate choice of $g(n)$, K can be bounded. It follows that the solutions to the congruence relation $a^{f(n)} - b^{f(n)} \equiv 0\ (mod\ n)$ is a bounded set, given by the solutions to $a^{f(1)+K} - b^{f(1)+K} \equiv 0\ (mod\ n)$. A rational-coefficient polynomial $f(n)$ which does not take integer values at all n, but which is integer at an arbitrarily large number of prime arguments, is sufficient for the proof. For a given polynomial function $f(n)$ and a non-zero value of $f(1)$, there are a finite number of prime divisors of $a^{f(1)+K} - b^{f(1)+K}$ and primes such that $a^{f(1)+K} - b^{f(1)+K} \equiv 0\ (mod\ p)$. Unless the function $f(r)$ has $r = 1$ as a zero, $a^{f(n)} \equiv b^{f(n)}\ (mod\ n)$ has a finite number of prime solutions when $f(r)$ is a polynomial with integer coefficients [28][29]. There, there must be an infinite number of primes such that

$$a^{f(p)} - b^{f(p)} \not\equiv \qquad (mod\ p) \tag{4.4}$$

for any function $f(r)$ which does not have a zero at $r = 1$. Indeed, $a^{f(p)} - b^{f(p)} \not\equiv 0\ (mod\ p)$ if it is prime. Choosing functions f_ℓ, $\ell = 1, 2, 3, ...$, such that $f_i(p_i) = f_j(p_j)$ it follows that

$$a^{f_\ell(p_\ell)} - b^{f_\ell(p_\ell)} \not\equiv 0 \qquad (mod\ p_\ell) \tag{4.5}$$

for $p_\ell > N_\ell$, $p' \neq a^{f_\ell(p_\ell)} - b^{f_\ell(p_\ell)}$. A set of functions $\{f_\ell\}$ with this property exists since the space of fractional-coefficient polynomials is $lim_{n\to\infty}\mathbb{Q}^n$. A bound on $f_\ell(1) + K_\ell$

can be obtained since the constraint on the polynomial fixes a single coefficient, and it implies the existence of an upper limit on the prime divisors of $a^{f_\ell(1)+K_\ell} - b^{f_\ell(1)+K_\ell}$ such that $N_\ell < \infty$ for all ℓ. The integers K_ℓ are less than p_ℓ, and moreover, the function f_ℓ may be chosen through the method of Lagrangian interpolation to have $K_\ell < K$, where K is a fixed upper bound as increasingly large primes p_ℓ are chosen. As $sup_\ell N_\ell < \infty$, $a^{f(p)} - b^{f(p)} \not\equiv 0 \ (mod\ p')$ for all primes $p' > sup_\ell N_\ell$, $f(p) \equiv f_\ell(p_\ell)$. Therefore, the primes satisfying $a^{f(p)} - b^{f(p)} \equiv 0 \ (mod\ p)$ and the prime divisors of $a^{f(p)} - b^{f(p)}$ will have an upper bouund of $sup_\ell N_\ell$, with the exception of $a^{f(p)} - b^{f(p)}$ if it is prime. The function $f_\ell(x)$ also should be selected such that it equals a prime at an arbitrary number of prime values of the argument. It can be obtained from a mapping of an arbitrary number of prime values to a subset of the arguments at which an irreducible integer-valued polynomial is prime, which can be achieved through Lagrangian interpolation (3.10). For example, polynomials such as $ax + b$, $gcd(a, b) = 1$, take prime values at an infinite number of integer arguments, whereas there exists a value of t such that the number of prime values of $x^k + t$, $k \geq 2$, is greater than any given finite lower bound [16][46]. An upper bound for the number of prime values of an irreducible polynomial for arguments less than x has been found [19], and the derivation can be extended to give a lower bound that tends to infinity as $x \to \infty$. Regarding the set of Mersenne primes as a Diophantine set, there exists a representation of these positive integers by a degree-914 polynomial in seven variables and a degree-26 polynomial in thirteen variables [21][41]. Suppose $f(x_\nu) = p'_\nu$, $\nu = 1, 2, 3, ...$, where the set $\{p_\nu\}$ is arbitrarily large and perhaps infinite and $f(x) = \sum_{k\geq 0} a_k x^k$. If a subset of the primes $\{p'_\nu\}$ does not coincide with the sequence of Mersenne prime indices, it can be mapped to this set of indices through a Lagrange interpolation function. If the set $\{x_\nu\}$ is infinite, there is a function h_∞ such that $h_\infty(p_\nu) = x_\nu$ for an infinite set of primes $\{p_\nu\}$. This function may be approximated by a polynomial of arbitrarily large but finite degree $h(x) = \sum_{k\geq 0} b_k x^k$ with rational coefficients which is bounded at finite values of the argument, since otherwise it would be discontinuous, and maps p_ν to x_ν for a given number of ν. The polynomial $\tilde{f} = f \circ h$, such that $\tilde{f}(p_\nu) = f(h(p_\nu)) = f(x_\nu) = p'_\nu$, als has rational coefficients $c_k = \sum_{j=0}^{k} a_j b_{k-j}$ and can be selected to belong to the set of functions $\{f_\ell\}$ which have prime values at an arbitrarily large number of prime arguments. When the set $\{x_\nu\}$ is arbitrarily large but finite, the polynomial h and the function h_∞ can be chosen to coincide. The integer $f_\ell(p_\ell)$ is a Mersenne prime index if the functions can be chosen such taht $f_i(p_i) = f_\ell(p_\ell)$ and $\{p_1, p_2, ...\}$ represents the entire set of primes. It follows that $f_1 = f \circ h_1 : \{2, 3, 5, ...\} \to \{p'_1, p'_2, p'_3, ...\}$, $f_2 = f \circ h_2 : \{3, 5, 7, ...\} \to \{p'_1, p'_2, p'_3, ...\}$, $f_3 = f \circ h_3 : \{5, 7, 11, ...\} \to \{p'_1, p'_2, p'_3, ...\}$,... . The range of values of the exponent for $a^t - b^t \not\equiv 0 \ (mod\ p)$, $p > sup_\ell N_\ell$, is given by $\cap_{\substack{\ell,p \\ p>sup_\ell N_\ell}} f_\ell(p) = \cap_\ell f_\ell(p)$ since the functions must satisfy $f_i(p_i) = f_j(p_j)$. It us not allowed to use another set of functions to determine the congruence relations for an exponent outside of this range because the theorem is applicable to $a^{f(n)} - b^{f(n)}$ for each function f and arbitrary integer values of f. Specifically, the use of an alternative set of functions $\{f'_\Upsilon\}$ would shift the value of $sup_\ell N_\ell$ to $sup_\Upsilon N'_\Upsilon$, and it would not be necessarily possible to bound the prime divisors

of $a^{F(p)} - b^{F(p)}$, $\{F\} = \{f_\ell, f'_\Upsilon, ...\}$.

Thus, for this set of primes p_ℓ, but not for every prime, $a^{f_\ell(p_\ell)} - b^{f_\ell(p_\ell)}$ does not have a proper divisor larger than a fixed bound $sup_\ell N_\ell$. For Mersenne numbers with prime index, $M_q = 2^q - 1$, the existence of divisors $p_j \leq sup_\ell N_\ell$ is feasible only if $2kq + 1 \leq sup_\ell N_\ell$. Thus, if $q > \frac{sup_\ell N_\ell - 1}{2}$, the functional set $\{f_\ell\}$ exists and $f_\ell(p_\ell) = q \ \forall p_\ell$, of $a^n - b^n$ for all $n \int \mathbb{Z},\ n \geq 2$, is consistent with the existence of a prime divisor $a - b \leq N_\ell$ for all ℓ. However, if $a = 2,\ b = 1$, the divisor is $a - b = 1$. Since $2^q - 1 \not\equiv 0\ (mod\ n)$ for all $n > 1$, $n \neq 2^q - 1$, the only integer divisors of $2^q - 1$ are 1 and $2^q - 1$, and $2^q - 1$ is prime.

The classification of polynomial and exponential functions may be used to prove the conjectured density of Mersenne primes. Let

$$\begin{aligned} s_n :\ & I^1 \to \{0, 1\} \\ s_n(x) = & \chi_P([f(n + x)]) \\ S_N^\psi :\ & I^1 \to \mathbb{R}_+ \\ S_N(x) = & \sum_{n=1}^{N} \frac{s_n(x)}{\psi(n)} \\ D_{\psi_1}^{\psi_2}(P, f; N) = & \frac{\sum_{1 \leq i \leq N} \frac{\chi_P([f(x+n)]}{\psi_1(n)}}{\sum_{1 \leq i \leq N} \frac{\chi_P(n)}{\psi_2(n)}} \end{aligned} \tag{4.6}$$

where $\psi,\ \psi_1,\ \psi_2$ are weighting functions and χ_P is the characteristic function for the set of prime numbers. It will be seen that the correct choice for ψ is usually

$$\psi(y) = \begin{cases} max\{log\ 2,\ log\ y\} & f \in \mathcal{F}_{pol}^* \\ y & f \in \mathcal{F}_{exp}^* \end{cases} \tag{4.7}$$

where

$$\begin{aligned} \mathcal{F}_{pol}^* = \{ay^k + \sum_{i=1}^{m} a_i y^{k_i};\ a > 0,\ k > k_1 > ... > k_m \geq 0 | f(0) \geq 0,\ f'(0) > 0,\ f'' > 0 \\ f''\ is\ monotonically\ increasing\} \\ \mathcal{F}_{exp}^* = \{e^{ky+\ell} + f(y);\ k > 0,\ f \in \mathcal{F}_{pol}^* \cup \{0\}\} \end{aligned} \tag{4.8}$$

This convention has been defined previously [28] except for a change in the lower bounds for $f(0)$ and $f'(1)$ in Eq.(4.8). Then, given that $2^y - 1 \in \mathcal{F}_{exp}^*$, switch on editor mode

$$S_N^\psi = \sum_{1 \leq n \leq N} \frac{\chi_P([f(x + n)])}{n} \tag{4.9}$$

and

$$S_N = S_N^{\psi}(0) = \sum_{1 \le n \le N} \frac{\chi_P([f(n)])}{n} \tag{4.10}$$

If $D_{har}^{log}(P, 2^y - 1; N)$ is defined with the weighting functions $\psi_1(y) = max\{log\ 2,\ log\ y\}$ and $\psi_2(y) = y$,

$$\begin{aligned} D_N^* &= (log\ 2) D_{\psi_1}^{\psi_2}(P, f; N)(0) = (log\ 2) \left(\sum_{1 \le n \le N} \frac{\chi_P(n)}{n} \right)^{-1} \sum_{1 \le n \le N} \frac{\chi_P([f(n)])}{n} \\ &= (log\ 2) \frac{S_N}{\sum_{1 \le n \le N} \frac{\chi_P(n)}{n}} \end{aligned} \tag{4.11}$$

Since $\sum_{p\ \ prime}^{p \le N} \frac{1}{p} = log\ log\ N + o(1)$ [27], and the probabilistic value of the density of the Mersenne prime indices [38] would be given by

$$lim_{N \to \infty} \frac{S_N}{log\ N} = \frac{e^{\gamma}}{log\ 2} \tag{4.12}$$

D_N^* is approximately $e^{\gamma} \frac{log\ N}{log\ log\ N}$ for known large Mersenne prime indices [37].

A proof of $\left| \frac{D_N^* log\ log\ N}{log\ N} - e^{\gamma} \right| < \epsilon$ for arbitrarily large N would provide the actual approximate value of the density of the Mersenne primes and the existence of arbitrarily many primes of this kind. If an irreducible rational-coefficient polynomial is chosen to approximate $2^y - 1$ over a certain interval, the weighting factor should be changed to $\psi(y) = y$, yielding

$$lim_{N \to \infty} \frac{S_N(P, f)}{log(N)} = \frac{1}{deg\ f} \prod_p \frac{p - \rho(p)}{p - 1} \tag{4.13}$$

where $\rho(p)$ is the number of solutions to $f(n) \equiv 0\ (mod\ p)$ [34]. When p increases, the number of solutions to $f(n) \equiv 0\ (mod\ p),\ 1 \le n \le N$, decreases rapidly and, as many of the terms in the product in Eq.(4.13) have the form $\frac{p}{p-1}$, approximate equality of $\frac{1}{deg\ f} \prod_p \frac{p - \rho(p)}{p-1}$ with the coefficient $\frac{e^{\gamma}}{log\ 2}$ may be obtained. The function $2^y - 1$ may be approximated by rational-coefficient polynomials of given order only over an inteval which includes the known Mersenne primes, whereas a method of intersecting polynomials at the next Mersenne prime described previously would be required for an approximation of the function throughout that value.

To determine the prime distribution of a function $[f(x + n)]$, the following intervals shall be defined.

$$\begin{aligned} I_{p,n} &= [f^{-1}(p) - n, f^{-1}(p+1) - n) \qquad p \in \mathcal{P} \\ I_{p.n}^{a,b} &= I_{p,n} \cap [a, b]. \end{aligned} \tag{4.14}$$

Since

$$\begin{aligned}\mu_t(I_{p,n}) &\sim |(f^{-1}(p+1)-n)-(f^{-1}(p)-n)| = |f^{-1}(p+1)-f^{-1}(p)| \\ &= \left|\left[f^{-1}(p)+(f^{-1})'(p)[(p+1)-p]+\frac{1}{2!}(f^{-1})''(p)[(p+1)-p]^2+...\right]-f^{-1}(p)\right| \\ &= \left|(f^{-1})'(p)+\frac{1}{2!}(f^{-1})''(p)+...\right|\end{aligned} \tag{4.15}$$

the Lebesgue measure of $I_{p,n}^{a,b}$, which is not empty if $\mathcal{P}_n(a,b) = \{p \in \mathcal{P} | f(n+a) \leq p \leq f(n+b)-1\}$ contains a prime, is given by

$$\begin{aligned}\mu(I_{p,n}^{a,b}) &= \frac{1}{f'(n+\Theta_p)} \qquad a \leq \Theta_p \leq b \qquad p \in \mathcal{P}_n^*(a,b) \\ \mathcal{P}_n^*(a,b) &= \{p \in \mathcal{P} | f(n+a) \leq p \leq f(n+b)-1\}\end{aligned} \tag{4.16}$$

Using the natural weighting, with $\psi(y) = 1$, it has been shown that

$$\begin{aligned}\int_0^1 S_N^{nat}(\mathcal{P};x)dx &= \sum_{n=1}^{N}\int_0^1 s_n(x)dx = \sum_{n=1}^{N}\sum_{p\in\mathcal{P}_n(0,1)}\mu(I_{p,n}^{0,1}) \\ &= \sum_{\substack{p\in\mathcal{P} \\ f(0)\leq p\leq f(N)}}[(f^{-1})'(p+\Theta_p)]+\mathcal{O}(1) = \sum_{\substack{p\in\mathcal{P} \\ f(0)\leq p\leq f(N)}}[(f^{-1})'(p)]+\mathcal{O}(1).\end{aligned} \tag{4.17}$$

Suppose that $f(y) = 2^y - 1$. Then

$$\sum_{p_n}(f^{-1})'(p_n) = \sum_{n\geq 2}\frac{1}{f'(n+\Theta_{p_n})} = \sum_{n\geq 2}\frac{1}{f'(f^{-1}(p_n))} = \sum_p \frac{1}{ln\ 2} = oneditormodety \tag{4.18}$$

It would appear that the index range of the sum is a presumption of the infinite extent of the sequence of Mersenne primes. However, the sufficiently fine subdivision of the unit interval, the infinitude of primes, the existence of a prime between a prime between between $f(n+a)$ and $f(n+b)-1$ for $a < b$ and sufficiently large n, given that $f(n+1) = 2f(n)+1$, and the overlapping of the subintervals $[a,b]$ with the inverse images under of f^{-1} of the primes and Mersenne numbers leads to the conclusion that the infinite sum (4.18) is direct evidence of the extent of the Mersenne prime sequence. It would follow that $lim_{N\to\infty}D_N^* \to e^{\gamma}\frac{log\ N}{log\ log\ N}$ continuously and monotonically, and this limit would be verification of the density of Mersenne primes.

This discussion clearly does not extend to integers of the form $a^y - 1$, $a \geq 3$, because these expressions can be trivially factored and the characteristic function $s_n(x) = \chi_{\mathcal{P}}([f(n+x)])$ then vanishes.

Appendix. Relations between the Mersenne Prime Indices

It may be verified that each Mersenne prime index can be expressed as a sum containing other Mersenne prime indices and having a particular choice of signs of the previous indices, with the possible exception of the previous exponent, which may be multiplied by a factor of 2. Given that $\{p'_n\}$ is the set of Mersenne prime indices,

$$
\begin{aligned}
p'_1 &= 2 \\
p'_2 &= 1 + 2 \\
p'_3 &= 1 - 2 + 6 \\
p'_4 &= 1 - 2 + 3 + 5 \\
p'_5 &= -1 - 2 - 3 + 5 + 2 \cdot 7 \\
p'_6 &= 1 - 2 + 3 - 5 + 7 + 13 \\
p'_7 &= 1 - 2 - 3 - 5 + 7 - 13 + 2 \cdot 17 \\
p'_8 &= 1 - 2 - 3 + 5 + 7 - 13 + 17 + 19 \\
p'_9 &= 1 + 2 - 3 - 5 - 7 + 13 + 17 - 19 + 2 \cdot 31 \\
p'_{10} &= 1 + 2 + 3 - 5 + 7 - 13 + 19 + 31 + 61 \\
p'_{11} &= 1 - 2 - 3 - 5 + 7 - 13 + 17 + 19 - 31 - 61 + 2 \cdot 89 \\
p'_{12} &= -1 + 2 + 3 + 5 - 7 - 13 + 17 + 19 - 31 - 61 + 87 + 107 \\
p'_{13} &= 1 + 2 - 3 - 5 + 7 + 13 - 17 - 19 + 31 + 61 + 89 + 107 + 2 \cdot 127 \\
p'_{14} &= 1 - 2 + 3 + 5 + 7 + 13 + 17 + 19 + 31 + 61 - 89 - 107 + 127 + 521 \\
p'_{15} &= 1 + 2 + 3 - 5 + 7 - 13 - 17 - 19 - 31 - 61 - 89 - 107 - 127 + 521 + 2 \cdot 607 \\
p'_{16} &= 1 + 2 + 3 + 5 - 7 - 13 + 17 + 19 + 31 + 61 + -89 - 107 - 127 + 521 + 606 \\
&\quad + 1279 \\
p'_{17} &= 1 + 2 - 3 - 5 + 7 + 13 + 17 + 19 - 31 - 61 + 89 + 107 + 127 - 521 - 607 \\
&\quad - 1279 + 2 \cdot 2203 \\
p'_{18} &= 1 + 2 - 3 - 5 - 7 + 13 + 17 - 19 - 31 + 61 + 89 + 107 - 127 + 521 - 607 \\
&\quad - 1279 + 2203 + 2281 \\
p'_{19} &= 1 - 2 - 3 - 5 + 7 - 13 - 17 + 19 + 31 + 61 + 89 + 107 - 127 - 521 - 607 \\
&\quad - 1279 - 2203 + 2281 + 2 \cdot 3217 \\
p'_{20} &= 1 + 2 + 3 - 5 - 7 + 13 + 17 + 19 + 31 + 61 + 89 - 107 + 127 + 521 - 607 \\
&\quad + 1279 - 2203 - 2281 + 3217 + 4253 \\
p'_{21} &= 1 + 2 - 3 + 5 - 7 - 13 + 17 + 19 + 31 + 61 + 89 + 107 + 127 - 521 + 607 \\
&\quad + 1279 - 2203 + 2281 + 3217 - 4253 + 2 \cdot 4423 \\
p'_{22} &= -1 + 2 + 3 - 5 - 7 + 13 - 17 + 19 - 31 - 61 + 89 + 107 - 127 - 521 + 607 \\
&\quad + 1279 - 2203 - 2281 + 3217 - 4253 + 4423 + 9689
\end{aligned}
$$

$$
\begin{aligned}
p'_{23} &= 1+2+3+5+7-13+17-19-31-61-89-107-127+521+607 \\
&\quad +1279+2203+2281+3217-4253-4423-9689+2\cdot 9941 \\
p'_{24} &= 1+2-3+5+7-13+17+19+31+61+89+107+127-521-607+1279 \\
&\quad +2203-2281+3217-4253+4423-9689+9941+11213 \\
p'_{25} &= 1+2+3+5-7-13+17+19+31-61+89+107+127+521+607 \\
&\quad +1279+2203+2281-3217+4253+4423-9689-9942-11213 \\
&\quad +2\cdot 19937 \\
p'_{26} &= 1+2+3-5-7+13+17+19-31-61+89+107-127+521-607 \\
&\quad +1279+2203-2281+3217+4253+4423+9689+9941-11213-19937 \\
&\quad +21701 \\
p'_{27} &= 1+2+3+5+7-13+17+19+31+61-89-107-127+521-607 \\
&\quad +1279+2203+2281-3217+4253+4423+9689+9941-11213+19937 \\
&\quad -21701+23209+44497 \\
p'_{28} &= 1+2-3+5-7-13-17-19-31-61-107-127+521+607 \\
&\quad +1279+2203+2281-3217+4253+4423+9689+9941-11213+19937 \\
&\quad -21701+23209+44497 \\
p'_{29} &= 1+2-3-5-7+13+17-19+31-61+89+107+127+521+607 \\
&\quad -1279+2203+2281+3217+4253+4423+9689+9941+11213-19937 \\
&\quad -21701-23209-44497-2\cdot 86243 \\
p'_{30} &= 1+2+3-5+7+13+17+19-31-61-89-107-127+521+607 \\
&\quad +1279-2203+2281+3217+4253+4423+9689+9941+11213+19937 \\
&\quad +21701-23209+44497-86243+110503 \\
p'_{31} &= 1-2+3+5-7-13+17-19+31+61-89-107+127-521-607 \\
&\quad +12179-2203+2281-3217-4253-4423+9689-9941+11213+19937 \\
&\quad -21701+23209-44497+86243+110503+132049+2\cdot 216091 \\
p'_{32} &= -2-3-5+7+13-17+19+31-61+89+107+127-521-607 \\
&\quad +1279-2203+2281+3217-4253+4423-9689+9941+11213-19937 \\
&\quad +21701+23209-44497+86243+110503+132049+2\cdot 216091 \\
p'_{33} &= -1-2-3-5-7-13-17+19-31+61+89+107+127-521+607 \\
&\quad -1279+2203-2281+3217+4253+4423-9689-11213-19937 \\
&\quad -21701-23209-44497-86243-110503-132049-216091 \\
&\quad +2\cdot 756839
\end{aligned}
$$

$$
\begin{aligned}
p'_{34} &= -2-3-5-7-13+17-19+31+61-89+107+127-521-607 \\
&\quad +1279-2203+2281-3217+4253+4423-9689+9941-11213+19937 \\
&\quad -21701+23209-44497+86243-110503+132049+216091 \\
&\quad -756839+2\cdot 859433 \\
p'_{35} &= 1-2-3+5-7-13+17+19-31+61-89+107+127-521+607 \\
&\quad +1279-2203-2281+3217-4253-4423+9689-9941-11213+19937 \\
&\quad +21701-23209-44497+86243+110503+132049+216091 \\
&\quad -756839-859433+2\cdot 1257787 \\
p'_{36} &= -2+3-5+7-13+17+19+31+61+89+107+127-521-607 \\
&\quad -1279+2203-2281+3217-4253+4423-9689+9941+11213-19937 \\
&\quad +21701+23209-44497+86243+110503+132049+216091 \\
&\quad -756839-859433+1257787+2\cdot 1398269 \\
p'_{37} &= -1-2-3+5+7-13-17+19+31-61-89-107-127+521-607 \\
&\quad -1279+2203+2281-3217-4253-4423+9689-9941+11213-19937 \\
&\quad +21701-23209-44497+86243-110503+132049-216091 \\
&\quad +756839-859433-1257787-1398269+\cdot 2\cdot 2976221 \\
p'_{38} &= 2+3-5+7+13-17-19-31+61+89-107-127-521-607 \\
&\quad +1279-2203+2281-3217+4253-4423+9689-9941-11213+19937 \\
&\quad -21701+23209-44497+86243+110503+132049+216091 \\
&\quad -756839+859433-1257787-1398269+2976221-2\cdot 3021377 \\
p'_{39} &= 1+2+3-5+7+13-17+19+31-61+89-107+127+521+607 \\
&\quad +1279-2203+2281-3217+4253-4423+9689-9941-11213+19937 \\
&\quad -21701-23209-44497+86243-110503+132049-216091 \\
&\quad +756839-859433+1257787-1398269+2976221-3021277 \\
&\quad +2\cdot 6972593 \\
p'_{40} &= -2-3-5-7+13+17+19+31-61-89+107+127-521-607 \\
&\quad -1279+2203-2281+3217-4253+4423-9689+9941-11213+19937 \\
&\quad -21701+23209-44497+86243-110503+132049+216091 \\
&\quad -756839-859433+1257787+1398269-2976221+3021377 \\
&\quad 6972593+2\cdot 134466917
\end{aligned}
$$

$$
\begin{aligned}
p'_{41} &= 1+2+3-5-7+13-17+19+31-61-89+107-127+521-607\\
&\quad -1279+2203-2281+3217-4253+4423-9689+9941+11213-19937\\
&\quad +21701+23209-44497+86243-110503+132049-216091\\
&\quad +756839-859433+1257787+1398269-2976221+3021377\\
&\quad -6972593-13466917+2\cdot 20996011\\
p'_{42} &= 2+3+5-7+13-17+19-31-61+89-107+127-521-607\\
&\quad +1279+2203+2281+3217-4253+4423-9689+9941+11213-19937\\
&\quad +21701+23209-44497+86243-110503-132049-216091\\
&\quad +756839-859433+1257787-1398269+29763221+3021377\\
&\quad +6972593-13466917-20996011+2\cdot 24036583\\
p'_{43} &= 1-2-3-5+7-13+17-19-31+61-89+107-127+521+607\\
&\quad -1279+2203-2281-3217+4253-4423+9689-9941+11213-19937\\
&\quad -21701-23209-44497-86243-110503-132049-216091\\
&\quad +756839-859433+1257787+1398269-2976221+31021377\\
&\quad -6972593-13466917+20996011-24036583+2\cdot 25964951\\
p'_{44} &= 2-3+5-7+13-17+19+31+61-89-107-127+521+607\\
&\quad +1279-2203-2281+3217-4253-4423+9689-9941+11213-19937\\
&\quad +21701+23209-44497+86243-110503-132049+216091\\
&\quad -756839+859433-1257787+1398269-2976221-3021377\\
&\quad -6972593+13466917+20996011-24036583-2594951\\
&\quad +2\cdot 30402457
\end{aligned}
\tag{A.1}
$$

Acknowledgements

Several of the properties of Mersenne prime indices in §2 were found in work on number theory at Universität Potsdam. The geometrical representation of the Mersenne number and several of the congruence conditions of §3 were obtained in research completed at the University of Syndey.

References

[1] E. Catalan, Sur la Théorie des Nombres Premiers, Turin, 1876, 11; Théorie des Nombres, 1891, 376.

[2] P. A. Cataldi, Trattato de Numeri Perfetto, Bologno, 1603.

[3] P. Chebyshev, Sur la Fonction qui Detérmine la Taotallité Inférieurs á unver Limite Donée, Mem. Préséntés l'Acad. Imp. Sci. St. Petersbourg par Divers Savants 6 (1851), 141-157.

[4] D. R. Curtiss, On Kellogg's Diophantine Problem, Amer. Math. Monthly 29 (1922), 380-387.

[5] S. Davis, On the Existence of a Non-Zero Lower Bound for the Number of Goldbach Partitions of an Even Integer, Int. J. Math. Mathemat. Sci. 2004: 15, 789-798.

[6] C. F. Eaton, Perfect Numbers in terms of Triangular Numbers, Solution to Problem 1482, Math. Mag. 69 (1996) 308-309.

[7] Euclid, Elements Book IX, Proposition 36, Opera 2, printed in Leipzig, 1884.

[8] L. Euler, Observationes De Theoretmate Quodam Fermatiano Aliisque ad Numeros Primos Spectantibus, Comm. Acad. Scientaiarum Petropolitanae 6 (1738), 103-107.

[9] L. Euler, Tractatus de Numerorum Doctrina Capita Sedecim Quae Supersunt, Ch. 3 (1756)

[10] P. de Fermat, letter to Mersenne, 1640, in Ouvres de Fermat, 2, Gauthier-Villars, Paris, 1894, 198-199

[11] P. de Fermat, letter to F. de Bessy, 1640, in Ouvres de Fermat, 2, Gauthier-Villars, Paris, 1894.

[12] B. Garrison, Polynomials with Large Numbers of Prime Values, Amer. Math. Monthly 97 (1990), 316-317.

[13] D. B. Gillies, Three New Primes and a Statistical Theory, Math. Comp. 18 (1964), 93-97.

[14] R. K. Guy, Unsolved Problems in Number Theory, Ch. 1, Springer-Verlag, New York, 2004.

[15] H. Heilbronn, Über die Vereilung der Primzahlen in Polynomen, Math. Ann. 104 (1931), 794-799.The study of the sum of the reciprocal divisors has been extended to lower bounds for odd perfect numbers [4].

[16] J. P. Jones, Diophantine Representation of Mersenne and Fermat Primes, Acta Arith. 35 (1979), 209-221.

[17] W. L. Kraft, Nova Acta Acad. Petrop. 12 (1801), 76.

[18] J. L. Lagrange, Recherch D'Arithmetique, Nuov. Mém. Acad. Berllin (1775), in Ouvres de Lagrange, Vol. 3, Gauthier-Villars, 1894, 695-795.

[19] D. H. Lehmer, An Extended Theory of Lucas Functions, Ann. Math. Ser. 2, 31 (1930), 419-448.

[20] E. Lucas, C. R. Acad. Sci. France 82 (1876), 167.

[21] E. Lucas, Théorie des Fonctions Numeriques Simplement Periodiques, Amer. J. Math. 1 (1878), 289-321.

[22] E. Lucas, Théorie des Nombres, Tome Premier, Gauthier-Villars, Paris, 1891.

[23] W. L. McDaniel, The Generalized Pseudoprime Congruence $a^{n-k} \equiv b^{n-k} \ (mod\ n)$, Comptes Rendus Math. Rep. Acad. Sci. Canada Vol. IX No. 3 (1987), 141-147.

[24] W. L. McDaniel, The Existence of Solutions of the Generalized Pseudoprime Congruence $a^{f(n)} \equiv b^{f(n)}$, Coll. Math. Vol. LIX (1990), 177-190.

[25] A. Makowski, Remark on Perfect Numbers, Elemente Math. 17 (1962) 109.

[26] M. Mersenne, Cogitata Physica - Mathematica, Preface, Chapter XIX, 1644.

[27] D. S. Mitrinovíc, J. Sandor and B. Crstici, Handbook of Number Theory, Mathematics and Its Applications, Vol. 351, Kluwer Academic Publishers, Dordrecht, 1996.

[28] Nichomachus, Introduction to Arithmetic, tr., by M. L. D'Ooge, F. E. Robbins and L. C. Karpinski, McMillan. New York, 1926.

[29] O. Ore, On the Averages of the Divisors of a Number, Amer. Math. Monthly 56 (1948), 615-619.

[30] E. Pecuttii, Pour L'Histoire des Sept Premiers Nombres Parfaits, Hist. Math. 16 (1989) 123-136.

[31] I. M. Pervouchine, Zap. Imp. Akad. Vol. 48 (1883).

[32] R. E. Powers, The Tenth Perfect Number, Amer. Math. Monthly 18 (1911), 195-197.

[33] P. Ribenboim, The New Book of Prime Number Records, Springer-Verlag, New York, 1996.

[34] F. Roesler, Über die Verteilung der Primzahlen in Folgen der Form $[f(x+n)]$, Acta Arith. XXXV (1979), 117-179.

[35] H. F. Scherk, Bemerkugen über die Bildung der Primzahlen aus Einander, J. Reine Angew. Math. 10 (1833), 201-208.

[36] W. Sierpinski, Elementary Theory of Numbers, Monografie Matematyczne Tom 42, Pańtwowe Wydawnictwo Naukawe, Warzwawa, 1964.

[37] W. Sierpinski, Les Binômes $x^2 + n$ les Nombres Premiers, Bull. Soc. Roy. Sci. Liege 33 (1964), 259-260.

[38] S. S. Wagstaff, Jr., Divisors of Mersenne Numbers, Math. Comp. 40 (1983), 385-397.

[39] J. Wu, Sur la suite des Nombres Premiers Jumeaux, Acta Arith. LV (1990), 365-388.

[40] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. 3 (1892), 265-284.