RFSC 04-02
Revised

A METHOD FOR GENERATING MERSENNE PRIMES AND THE EXTENT OF THE SEQUENCE OF 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, and that all Mersenne prime indices less than or equal to 19 have the form $p_1' + p_2' - 1$, with $2^{p_1'} - 1$ and $2^{p_2'} - 1$ both being primes. 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 differences of powers with polynomial exponents are used to prove the infinite extent of the sequence of Mersenne primes.

MSC: 11N13, 11N32, 11P83

1. Introduction

The Lucas-Lehmer test [11][12], together with several characteristics of prime divisors of Mersenne numbers, which are valid for all Lucas sequences can be used to determine theoretically whether the integer 2^n-1 is prime. The congruence modulo 2^n-1 is satisfied by the known Mersenne primes, although the difficulty of the computation increases for larger 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 may be solved without the 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 §2that since every prime exponent p has the form p_1+p_2-1, where p_1 and p_2 are prime, with several conditions being given for $2^{p_1+p_2-1}-1$ to be composite, 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 the index of a composite Mersenne number.

The Mersenne numbers have a geometrical representation which may be used to derive 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 common denominator of the initial term and the difference can be equated with $ord_{2^m-k}(k)$ for some m, k, so 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 congruence 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.

A proof of the existence of infinitely many Mersenne primes is given in §4. 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 demonstrate that there are an infinite number of values of n for which 2^n-1 does not have a proper prime divisor.

2. The Exponents of Mersenne Numbers and Arithemetical Progressions

There are two infinite sequences, of Mersenne numbers with 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 numbers continues indefinitely.

Since $6n+1$ can be factorized only if n has the form $6xy \pm (x+y)$ with x and y, 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 $2^p - (6z+1) = (6x \pm 1)(6y \pm 1)$, consider two primes p_1 and p_2 such that

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

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

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

It can be checked that the known Mersenne prime indices greater than 31 cannot be expressed as p_1+p_2-1 for two primes p_1, p_2 such that both $2^{p_1}-1$ and $2^{p_2}-1$ are prime. If $z_1 \neq 0$, and $2^{p_1}-1$ is prime, while z_2 is set equal to zero, so that $2^{p_2}-1$ 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 equation (2.4) with $\gamma_1 = \gamma_2 = \gamma_3 = 1$. If p_1 is a given Mersenne prime index, it can be conjectured that $p_1 - 1$ can 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 $\prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)$ [16][23], and

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

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 exists two primes q_1, q_2 such that $2N = q_1 + q_2$ if the Goldbach conjecture [7][8] 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 can be assumed that this property holds for all integers $1 \leq \tilde{N} < \bar{N}$ 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 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 $q_3 > \bar{q}_1,\ q_4 < \bar{q}_2 + 2$ 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 $2N + 2\imath$, $\imath \geq 2$, 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 $q_4 + k_2 < 2\bar{N}$ when $\bar{q}_2 - q_4 - k - k' > 0$ and $\bar{q}_2 < 2\bar{N}$. Suppose that the equality between $q_4 + k_2$ 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

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

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. The lesser prime in the difference satisfies the inequality $q_4 - \bar{q}_2 - k - k' < 2\bar{N}$ since $q_4 - \bar{q}_2 < q_3 - \bar{q}_2 < \bar{q}_1 - \bar{q}_2 = 2\bar{N}$.

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

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. This property can be verified for the

following pairs of prime indices (p_1, p_2):

$(3,11); (7,11); (3,29); (19,43); (31,59); (61,47); (61,67); (89,433); (61,547);$
$(607; 673); (2203,937); (2281,1973); (4253,5347); (4253,6961); (2281,17657); (89,21613);$
$(2281,20929); (3217,41281); (9941,76303); (607,109897); (44497,87553); (23209; 192883);$
$(132049,624791); (19937,839497); (132049,1125739); (86243,1312027); (86243,2889979);$
$(21701,3049677); (3071377,3901217); (216091,13250827); (110503; 20885509)$
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, $\{(2,2); (3,3);$
$(3,5); (7,7); (5,13); (3,17); (7,13); (13,19)\}$, complement the larger set when
$p_1 + p_2 - 1 = 3, 5, 7, 19$.

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

$$\begin{aligned} h_1 &= 6x_1y_1 + (x_1 + y_1) \qquad h_2 = 6x_2y_2 + (x_2 + y_2) \\ w_1 + w_2 &= 3(x_1 + y_1 + z_1)(x_2 + y_2) + (x_1 + y_1 + z_1) + (x_2 + y_2) \\ w_1w_2 &= 18x_1y_1x_2y_2 + 3x_1y_1(x_2 + y_2) + 3x_2y_2(x_1 + y_1 + z_1) + (x_1y_1 + x_2y_2) \end{aligned} \tag{2.9}$$

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

$$\begin{aligned} h_1 &= 6x_1y_1 + (x_1 + y_1) \qquad h_2 = 6x_2y_2 - (x_2 + y_2) \\ w_1 + w_2 &= -3(x_1 + y_1 + z_1)(x_2 + y_2) + 6(x_1y_1 + x_2y_2) + (x_1 + y_1 + z_1) - (x_2 + y_2) \\ w_1w_2 &= 18x_1y_1x_2y - 2 - 3x_1y_1(x_2 + y_2) + 3x_2y_2(x_1 + y_1 + z_1) + (x_1y_1 + x_2y_2) \end{aligned} \tag{2.11}$$

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

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

$$2u^2 - 2(h_1 + z_1 + h_2)u + (h_1 + z_1)h_2 = 0 \tag{2.13}$$

and

$$u = \frac{1}{2}\left[h_1 + z_1 + h_2 \pm \sqrt{(h_1 + z_1 + h_2)^2 - 2(h_1 + z_1)h_2}\right] \tag{2.14}$$

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,

$$\begin{aligned} u+v &= \kappa_1(h_1+z_1)h_2+\kappa_2(h_1+z_1+h_2) \\ uv &= \kappa_3(h_1+z_1)h_2+\kappa_4(h_1+z_1+h_2) \end{aligned} \tag{2.15}$$

with

$$\begin{aligned} \kappa_1+6\kappa_3 &= 3 \\ \kappa_2+6\kappa_4 &= 1 \\ \kappa_1,\kappa_2,\kappa_3,\kappa_4 &\in \mathbb{Q} \end{aligned} \tag{2.16}$$

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

Additional constraints can be placed on h_1+z_1, h_2 as the equality of $6(3(h_1+z_1)h_2+(h_1+z_1)+h_2)+1$ with $2^{p_1+p_2-1}-1$ would imply congruence conditions. First, after division by 2, it follows that either $h_1+z_1\equiv 0\ (mod\ 4),\ h_2\equiv 5\ (mod\ 8),\ h_1+z_1\equiv\ 5(mod\ 8),\ h_2\ \equiv 0\ (mod\ 4),\ h_1+z_1\equiv 1\ (mod\ 4),\ h_2\equiv 3\ (mod\ 4),\ h_1+z_1\equiv\ 3(mod\ 4),\ h_2\equiv 1\ (mod\ 4)$. Secondly, $3(h_1+z_1)h_2+(h_1+z_1)+h_2\equiv\frac{2^n-1}{3}\ (mod\ 2^n)$, *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*.

3. On a Geometrical Representation of the Mersenne Number

Division of a triangular array of sites representing the Mersenne number 2^n-1 into more than two approximately equal parts defines the partition of 2^n-1 into the sum of at least three nearly equal positive integers. This type of partitioning provides a geometrical method for determining whether a Mersenne number is composite, since it can be factored if it is the sum of at least three consecutive numbers [18], as $K|[I+(I+1)+(I+2)+...+(I+(K-1))]$ when K is odd.

Suppose that the triangle is divided into K parts. The site located at a fraction of the distance along the m^{th} level, $\frac{\bar{m}}{2^m-1}\cdot l_m$, will be included in the j^{th} triangle if

$$\frac{(j-1)(2^m-1)}{K}\le\bar{m}\le\frac{j(2^m-1)}{K} \tag{3.1}$$

The number of sites included in the j^{th} triangle is

$$N_m^K\ =\ \left[\frac{j(2^m-1)}{K}\right]\ -\ \left\{\frac{(j-1)(2^m-1)}{K}\right\}\ +\ 1 \tag{3.2}$$

If the partition includes a site on the i^{th} level, where $i\le n-1$, then $K|2^m-1$ for some $m|i$, and the divisor function τ_2 can be defined by $\tau_2(i,K)=1+ord\{m|m\neq 0,\ m|i,\ K|2^i-1\}$.

The notation $[m]$ will be used to denote the set of integers which are multiples of m less than n, beginning with m and ending with i.

Consider the Lucas sequence $U_n(a,b) = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ with $a = \alpha + \beta$, $b = \alpha\beta$ and $U(3,2) = 2^n - 1$. Since $gcd(U_m, U_n) = U_\nu$ where $\nu = gcd(m,n)$, $K|U_\nu$ if $K|U_m$ and $K|U_n$. A partition of the triangle into K equal regions will intersect the site at the ν^{th} level and all three sites will belong to the same set. Continuing this process, it follows that there is a minimum value m_0 such that the set $[m_0]$ contains all integers $1 < m \leq n-1$ for which $K|2^m - 1$. Denoting the final integer in this sequence to be i, the number of shared sites is $1 + (K-1)(\tau_2(i,K) - 1)$ and the number of overcounted sites is $(K-1)\tau_2(i,K)$.

The sites are distributed approximately equally amongst the K triangles. However, at a particular level m, a certain set of triangles $\{T_{j'}\} \subset \{T_j\}$ will contain an extra site. If $2^m - 1 \equiv K_m \ (mod\ K)$, there will be indices $j_{m,s}$, $s = 0, 1, ..., K_m$, $j_{m,0} = 1$, $j_{m,1} = \{\frac{K}{K_m}\}, j_{m,2} = \{\frac{2K}{K_m}\}, ..., j_{m,K_{m_K}-1} = \{\frac{(K_m-1)K}{K_m}\}, j_{m,K_m} = K$ such that $T_{j_{m,s}}, s \geq 1$ contains an extra site. Since $2^{m+1} - 1 \equiv 2K_m + 1 \ (mod\ K)$, an additional site is located in each of the triangles $T_{j_{m+1,s}}$ with $j_{m+1,0} = 1, j_{m+1,1} = \{\frac{K}{2K_m+1}\}, j_{m+1,2} = \{\frac{2K}{2K_{m_K}+1}\}, ...,$ $j_{m+1,2K_m} = \{\frac{2K_mK}{2K_m+1}\}, j_{m+1,2K_m+1} = K$.

Let m_K be the first integer such that $2^m - 1 > K$ or $2^{m_K} > K + 1 > 2^{m_K - 1}$ so that $m_K = \{log_2(K+1)\}$ and

$$2^{m_K} - 1 \equiv K_{m_K} \ (mod\ K) \qquad\qquad 1 \leq K_{m_K} \leq K \tag{3.3}$$

At level m_K, the 2^{m_K} sites distributed amongst the K triangles produce an extra $K_{m_K} + 1$ sites.

Moreover, given a sequence of congruence relations $2^{m_K} \equiv K_{m_K} + 1 \ (mod\ K)$, $2^{m_K+1} \equiv 2(K_{m_K} + 1) \ (mod\ K)$,...,$2^{n-1} \equiv 2^{n-1-m_K}(K_{m_K} + 1) \ (mod\ K)$, the number of extra sites from levels $m_K, ..., n-1$ is

$$\sum_{i=m_K}^{n-1} 2^{(i-m_K)}2^{m_K} = 2^{m_K}\Bigg[(2^{m_K} - 1) + 2^{m_K}((2^{m_K} - 1) + \\ ... + 2^{m_K}\left((2^{m_K} - 1) + 2^{m_K}\sum_{i=rm_K}^{n-1} 2^{i-rm_K}\right)\Bigg] \tag{3.4}$$

where r is an integer such that $rm_K < n - 1 < (r+1)m_K$, which is congruent to

$$\begin{aligned}(K_{m_K} + 1)\Bigg[&K_{m_K} + (K_{m_K} + 1)(K_{m_K} + (K_{m_K} + 1)(K_{m_K} + (K_{m_K} + 1)(K_{m_K} + \\ &... + (K_{m_K} + (K_{m_K} + 1) \cdot (2^{n-rm_K} - 1))\Bigg] \qquad (mod\ K) \\ = \ & 2^{n-rm_K}(K_{m_K} + 1) - (K_{m_K} + 1) \qquad (mod\ K)\end{aligned} \tag{3.5}$$

When $2^i < K$, there will be either 0 or 1 site in the i^{th} triangle and the number of extra sites from levels 0 to $m_K - 1$ is

$$\sum_{i=0}^{m_K-1} 2^i \;=\; 2^{m_K} - 1 \;\equiv\; K_{m_K} \qquad (mod\ K) \tag{3.6}$$

so that from levels 0 to $n-1$, they total

$$2^{n-rm_K}(K_{m_K}+1) - 1 \qquad (mod\ K) \tag{3.7}$$

Compositeness of the Mersenne number requires that the entire sum is a sum of consecutive integers. The Mersenne number therefore will be composite if the number of extra sites, not overcounting shared sites, is congruent to the number $\frac{K(K+1)}{2}$ modulo K for some integer $K \geq 3$.

The congruence relations may be verified for several composite Mersenne numbers: $n = 11,\ K = 23,\ m_K = 5,\ K_{m_K} = 8,\ r = 2,\ 2^{n-rm_K}(K_{m_K}+1)^r - 1 = 161 \equiv 0 \equiv \frac{K(K+1)}{2}\ (mod\ 23)$; $n = 23,\ K = 47\ m_K = 6,\ K_{m_K} = 16,\ r = 3,\ 2^{n-rm_K}(K_{m_K}+1)^r - 1 = 157215 \equiv 0 \equiv \frac{K(K+1)}{2}\ (mod\ 47)$; $n = 29,\ K = 233,\ m_K = 8,\ K_{m_K} = 22,\ r = 3,\ 2^{n-rm_K}(K_{m_K}+1)-1 = 389343 \equiv 0 \equiv 0 \equiv \frac{K(K+1)}{2}\ (mod\ 233)$; $n = 37,\ K = 223,\ m_K = 8,\ K_{m_K} = 32,\ r = 4,\ 2^{n-rm_K}(K_{m_K}+1) - 1 = 37949471 \equiv 0 \equiv \frac{K(K+1)}{2}$;$n = 41,\ K = 13367,\ m_K = 14,\ K_{m_K} = 3016,\ r = 2,\ 2^{n-rm_K}(K_{m_K}+1) - 1 = 74565951487 \equiv 0 =\equiv \frac{K(K+1)}{2}\ (mod\ 13367)$; $n = 43,\ K = 431,\ m_K = 9,\ K_{m_K} = 80,\ r = 4,\ 2^{n-rm_K}(K_{m_K}+1) - 1 \equiv 0 \equiv \frac{K(K+1)}{2}\ (mod\ 431)$.

When $n - 1 - m_K = h\ ord_K(2) + r_2(n-1,K),\ 1 \leq r_2(n-1,K) \leq ord_K(2) - 1$, the total number of extra sites is

$$\begin{aligned} &\sum_{i=0}^{m_K-1} 2^i \;+\; \sum_{t=0}^{h\ ord_K(2)+r_2(n-1,K)} 2^t(K_{m_K}+1) \\ &\quad= \; 2^{m_K} - 1 + (2^{h\ ord_K(2)+r_2(n-1,K)+1} - 1)(K_{m_K}+1) \\ &\quad\equiv \; (2^{r_2(n-1,K)+1} - 1)(K_{m_K}+1) \;-\; 1 \qquad (mod\ K) \end{aligned} \tag{3.8}$$

If h congruence cycles of the doubling map are completed between levels m_K and $n-1$, then the total number of extra sites is

$$\begin{aligned} \sum_{i=0}^{m_K-1} 2^i \;+\; \sum_{t=0}^{h\ ord_K(2)} 2^t(K_{m_K}+1) \;&=\; 2^{m_K} - 1 + (2^{h\ ord_K(2)+1} - 1)(K_{m_K}+1) \\ &\equiv 2K_{m_K} + 1\ (mod\ K) \end{aligned} \tag{3.9}$$

for odd K.

Since $\frac{K(K+1)}{2} \equiv 0$ when K is odd, a necessary condition for compositeness of the Mersenne number is

$$2^{1+\{log_2(K+1)\}} - 2^{1+log_2 K} - 1 \equiv 0 \qquad (mod\ K) \tag{3.10}$$

which implies that $2^{1+\{log_2(K+1)\}} - 2^{1+log_2 K} = K+1$. This condition has the solutions $K = \frac{4^m-1}{3}$, $m \geq 2$. The Mersenne number is composite when n equals $1+\{log_2(K+1)\}+ h\ ord_K(2)$ and $K = \frac{4^m-1}{3}$, $m \geq 2$. The exponents in this sequence are all even because $\{log_2\left(\frac{4^m+2}{3}\right)\} = 2m-1$ and $ord_{\frac{4^m-1}{3}}(2) = 2m$.

Since $K_{m_K} = 2^{\{log_2(K+1)\}} - (K+1)$, the congruence relation for a composite Mersenne number is

$$2^{n-rm_K}(2^{\{log_2(K+1)\}} - K)^r - 1 \equiv 0 \qquad (mod\ K) \tag{3.11}$$

Let $x = n - r\{log_2(K+1)\}$ and $K = 2^m - k$. Then the existence of integer solutions (x, r, k, m) to the condition

$$2^x k^r - 1 \equiv 0 \qquad (mod\ 2^m - k) \qquad\qquad k \leq 2^{m-1},\ m \in \mathbb{Z} \tag{3.12}$$

is sufficient for the compositeness of $2^n - 1$. If (x, r, k, m) is a solution to equation (3.12), then $(x, r + h\ ord_{2^m-k}(k), k, m)$ also is a solution. It follows that $2^n - 1$ is composite if $n = (x + r\{log_2(2^m + 1 - k)\}) + ord_{2^m-k}(k)\{log_2(2^m + 1 - k)\}h$. However,

$$(2^m - k)^n \ = \ 2^{mn} - \binom{n}{1} 2^{m(n-1)}k \ + \ ... \ + \ (-1)^n k^n \tag{3.13}$$

and $2^{mn} - 1 \equiv 0\ (mod\ K)$ if $2^n - 1 \equiv 0\ (mod\ K)$. The last equation implies that

$$\begin{aligned} 1 - \binom{n}{1} 2^{m(n-1)}k \ \ \binom{n}{2} 2^{m(n-2)}k^2 \ + \ k^2 \ + \ ... \ + \ (-1)^n k^n & \\ \equiv \ 1 \ + \ \left[-\binom{n}{1} + \binom{n}{2} + ... + (-1)^n \right] k^n & \\ = \ 1 - k^n \ \equiv \ 0 \qquad (mod\ 2^m - k) & \end{aligned} \tag{3.14}$$

and $ord_K(k)|n$. Therefore $ord_K(k)|x + r\{log_2(K+1)\}$ and the arithmetic sequence generates composite numbers.

When $2^n - 1$, $n > 6$, it has a proper primitive divisor [2][4][24], and there exista a factor which has the form $2^m - k$, $m \not| n$, $1 < k \leq 2^{m-1}$. The set of integers $E_n = \{e | 2^e - 1 \equiv 0\ (mod\ 2^m - k),\ m \not| n,\ 1 < k \leq 2^{m-1},\ \{ord_{2^m-k}(k) = n\}$ contains the integer n when it is the exponent of a composite Mersenne number. The set of exponents of composite Mersenne numbers will be $\cup_n E_n$ which contains $O = \cup_n O_n = \cup_n \{ord_{2^{m_n}-k_n}(k_n) = n\}$. The product of two integers in O also belongs to O, and any multiple of an integer in O is an element of O. $\{O_n\}$ spans $\cup_n E_n$ because every element of E_n is a multiple of n. The complement of the set of integers in O would have either $ord_K(k) = 1$ or $ord_K(k) \neq p$

for any $K \geq 3$ and $1 < k \leq 2^{p-1}$ with $K \not| 2^p - 1$, $2^p - k \not| 2^p - 1$, where p is the prime exponent, or it consists of integers belongs to sequences of the type $a + bn$, $gcd(a, b) = 1$, where $ord_K(k) \neq a$ for any $K \geq 3$ and $1 < k \leq 2^{p-1}$ satisfies the same divisibility conditions.

Suppose further that p_1 and p_2 are two prime indices such that

$$\begin{aligned} 2^{p_1} - 1 &\equiv x_1 \qquad (mod\ 2^m - k_1) \\ 2^{p_2} - 1 &\equiv x_2 \qquad (mod\ 2^{m'} - k_2) \end{aligned} \tag{3.15}$$

and $p_1 + p_2 - 1$ is prime. Then

$$\begin{aligned} 2^{p_1+p_2-1} - 1 \ &\equiv \ \frac{x_1x_2 + x_1 + x_2 + c_1c_2 - 1}{2} \ + \ \frac{c_1}{2}(1 + x_2)(2^m - k_1) \\ &\quad + \ \frac{c_2}{2}(1 + x_1)(2^{m'} - k_2) \qquad (mod\ 2^{m+m'-1} - k_3) \\ k_3 \ &= \ 2^{m-1}k_2 + 2^{m'-1}k_1 - \frac{k_1k_2 - 1}{2} \end{aligned} \tag{3.16}$$

Allowing for the shift $x_1 \rightarrow x_1 + \alpha(2^m - k_1)$, $c_1 \rightarrow c_1 - \alpha$, $x_2 \rightarrow x_2 + \beta(2^{m'} - k_2)$, $c_2 \rightarrow c_2 - \alpha$, the congruence relation becomes

$$\begin{aligned} 2^{p_1+p_2-1} - 1 \ &\equiv \ \frac{x_1x_2 + x_1 + x_2 + (c_1 - \alpha)(c_2 - \beta) - 1}{2} \\ &\quad + \ \frac{1}{2}c_1(1 + x_2)(2^m - k_1) \ + \ \frac{1}{2}c_2(1 + x_1)(2^{m'} - k_2) \\ &\quad + \ \frac{1}{2}(c_1\beta + c_2\alpha - \alpha\beta)(2^m - k_1)(2^{m'} - k_2) \qquad (mod\ 2^{m+m'-1} - k_3) \end{aligned} \tag{3.17}$$

Expressing this quadratic form as a product of linear terms,

$$\begin{aligned} &\left[(c_1\beta + c_2\alpha - \alpha\beta)\left\{(2^m - 1) + c_2(1 + x_1)(c_1\beta + c_2\alpha - \alpha\beta)^{-1}\right\}\right] \\ &\quad \left\{(2^{m'} - k_2) + c_1(1 + x_2)(c_1\beta + c_2\alpha - \alpha\beta)^{-1}\right\} \\ &\quad \equiv \ c_1c_2(c_1\beta + c_2\alpha - \alpha\beta)^{-1}(1 + x_1)(1 + x_2) \\ &\quad - ((1 + x_1)(1 + x_2) + c_1c_2 - (c_1\beta + c_2\beta_\alpha\beta)) + 1 \ \ (mod\ 2^{m+m'-1} - k_3) \end{aligned} \tag{3.18}$$

it follows that $2^{p_1+p_2-1} - 1$ can be factored when there are integer solutions for x_1, x_2, α and β modulo $2^{m+m'-1} - k_3$, which suggests that the set of prime exponents of composite Mersenne numbers is infinite.

4. Exponential Congruence Relations for the Sequence of Mersenne Primes

The existence of an infinite number of Mersenne primes is known to be connected to the irrationality of the zeta function for a S-integer dynamical system [5]. For a dynamical system defined by a function $F_n(\phi) = \{x \in M | \alpha^n x = x\}$, with $\alpha : M \rightarrow M$ being a continuous map, the dynamical zeta function is

$$\zeta_\phi(z) \ = \ exp\left(\sum_n \ |F_n(\phi)| \frac{z^n}{n}\right) \tag{4.1}$$

When $\{\frac{1}{n} log|F_n(\phi)|\}_{n=1}^{\infty} \ = \ \left\{\left(1 - \frac{1}{q}\right) h(\phi) \middle| q \in \mathbf{N}\right\} \cup \{h(\phi)\}, \ h(\phi) = log\ 2,$
$lim_{n\rightarrow\infty}|F_n(\phi)| = 2^{n\left(1-\frac{1}{q}\right)}$ and

$$\begin{aligned} \zeta_\phi(z) \ &= \ exp\left(\sum_n \ \frac{(2^{\left(1-\frac{1}{q}\right)}z)^n}{n}\right) \ + \ finite\ term \\ &= \frac{1}{1 - 2^{\left(1-\frac{1}{q}\right)}z} \ + \ finite\ term \end{aligned} \tag{4.2}$$

which has an infinite number of poles in the unit disk at $\{z\} = \left\{\frac{1}{2}, 1, \frac{1}{\sqrt{2}}, \frac{1}{2^{\frac{2}{3}}}, \frac{1}{2^{\frac{3}{4}}}, ...\right)\}$ and is therefore irrational.

Let $z = 2^{-s}$. Then

$$\zeta_\phi(z(s)) \ = 1 \ + \ 2^{\left(1-\frac{1}{q}\right)-s} \ + \ \left(2^{\left(1-\frac{1}{q}\right)-s}\right)^2 \ + \ ... \tag{4.3}$$

From the set of Mersenne prime indices $S = \{p | 2^p - 1 \ is \ prime\}$, the set $\bar{S} = \{\sum_i p_i | p_i \in S\}$. All of the powers of $t = 2^{1-s}$ in the zeta function for the group $G = \prod_{p\in S} \ PSL_2(p)$, $\zeta_{G,2}(s) = \prod_{p\in S}(1 + t^p)$ [19], with the exception of different coefficients, can be obtained from $\zeta_\phi(z)$ by selecting those terms arising from the set $\bar{S}$

$$\zeta_\phi(z(s)) \ \rightarrow \ 1 \ + \ \sum_{n\in\bar{S}} \ 2^{n(1-s)-\frac{n}{q}} \ \underset{q \rightarrow \infty}{\longrightarrow} \ 1 \ + \ \sum_{n\in\bar{S}} \ 2^{n(1-s)} \tag{4.4}$$

which is a rational function of $z = 2^{-s}$.

If $n_g = 2^{g-1}(2^g - 1)$, then $n_g = 4n_{g-1} + 2^{g-1}$ follows from the decomposition of the Mersenne number $2^g - 1$ into $2^{g-1} - 1$ and 2^{g-1}. When $2^g - 1$ is a Mersenne prime, this is the only possible expression in terms of a sum of consecutive integers. If a prime other than the factor $2^g - 1$ is used, this recursion relation is not valid. Similarly, composite integers other than 2^{g-1} can be decomposed into three or more addends, which implies that there are additional factors giving rise to a sum-of-divisors function $\sigma(N)$ not satisfying $\frac{\sigma(N)}{N} = 2$.

The factor of 4 in the recurrence relation for n_g is a reflection of the equivalence between these integers and the number of odd spin structures on a genus-g Riemann surface. A spin structure $\mathcal{S}_\xi$ on Σ, which is a holomorphic line bundle $\mathcal{L}$ such that $\mathcal{L}^{\otimes 2} = \mathcal{K}$, the cotangent bundle, may also be viewed as a quadratic refinement $q_\xi : H_1(\Sigma, \mathbb{Z}_2) \to \mathbb{Z}_2$, of an intersection form $\sigma(mod\ 2) : H_1(\Sigma, \mathbb{Z}_2) \otimes H_1(\Sigma, \mathbb{Z}_2) \to \mathbb{Z}_2$ [22] satisfying the property $q_\xi(t_1 + t_2) = q_\xi(T_1) + q_\xi(t_2) + \sigma(mod\ 2)(t_1, t_2),\ t_1, t_2 \in \mathbb{Z}_2$. The Atiyah invariant, the dimension, mod 2, of the holomorphic line bundle defined by the spin structure on the surface Σ, which is zero $2^{g-1}(2^g+1)$ times and equal to $2^{g-1}(2^g-1)$ times [1][10]. Defining $\Gamma_g^+$to be the subgroup of the mapping class grojup Γ_g which leaves invariant a quadratic refinement q_ξ corresponding to an even spin structure $\mathcal{S}_\xi$ and an even theta characteristic ξ, the even spin moduli space is $M_g+ = T_g/\Gamma_g^+$. Similarly, if Γ_g^- is the subgroup of the mapping class group which leaves invariant an odd spin structure, then $M_g^- = T_g/\Gamma_g^-$ is the odd spin moduli space. The counting of odd spin structures on a Riemann surface is based on a binary system, because the number of Dirac zero modes is either 0 or 1 mod 2 and it is additive when surfaces of genus g_1 and g_2 are joined. Since there are one odd and three even spin structures on a torus, the odd spin structures at genus $g-1$ can be combined with any of the three even spin structures at genus 1, and the even spin structures at genus $g-1$ can be combined with the odd spin structure at genus 1 to produce odd spin structures at genus g. This reveals the singlet-triplet structure underlying the binary system and the number of ways of combining odd and even structures for each handle to produce an overall spin structure is $1+\binom{g}{2}\cdot 3^2+\binom{g}{4}\cdot 3^4+...+\binom{g}{g-1}\cdot 3^{g-1} = \frac{(1+3)^g+(1-3)^g}{2}$ $= 2^{g-1}(2^g-1)$ when g is odd. The properties of the set of odd spin structures, when 2^g-1 is a Mersenne prime, which might continue indefinitely, shall be described subsequently.

At genus g, all odd spin structures can be generated by the application of modular transformation to a set of 2^{g-1} spin structures. The Ramond sector R consists of 2^g structures with genus-one components that are either $(+-)$ or $(++)$. By adding the genus-one components and computing the overall parity of the theta characteristic defined by the genus-g spin structure, it can be deduced that there are 2^{g-1} even and 2^{g-1} odd spin structures in the Ramond sector. At genus one, the modular group $PSL(2;\mathbb{Z})$, generated by $\tau \to \tau + 1$ and $\tau \to -\frac{1}{\tau}$, where τ is the period of the torus, interchanges the even spin structures $\{(+-), (-+), (--)\}$ and leaves invariant the odd spin structure $(++)$. One method for generating the remaining odd spin structures is the application of products of parity-changing genus-one transformations, acting on different handles, to the subset of odd spin structures R_0 in the Ramond sector [6]. Denoting the modular transformations by ρ_r, $r = 1, ..., 3^g - 2^g - 1$, it follows that $R_0 \cup \cup_r \rho_r(R_0)$ contains all of the odd spin structures at genus g.

However, this techinique is not based on the use of the minimal number of transformations for generating these spin structures. First, the genus-g spin structure $(++++...++)$ is left invariant by all ρ_r and therefore it appears in every set $\rho_r(R_0)$. Secondly, a genus-

one modular transformation acting on only one handle alters 2^{g-2} spin structures in R_0, while modular transformations acting on only one handle alters 2^{g-2} spin structures in R_0, while a product of genus-one modular transformations acting on ℓ handles alters $2^{g-2} + 2^{g-3} + ...2^{g-\ell} = 2^{g-\ell}(2^\ell - 1)$ spin structures. since $2^{g-\ell}$ spin structures are unchanged, many of the spin structures are counted repeatedly in the union $R_0 \cup \cup_r \rho_r(R_0)$. The presence of a fixed spin structure $(+++++...++)$ is an indication of the inclusion of the modular transformations ρ_r in the group Γ_g^-.

Since there are other modular transformations, belonging to the group Γ^+, which alter all of the spin structures in R_0, they can be used to generate the odd spin structures with minimal overlap between between the different sets. If there exist modular transformations which induce no overlap, they may be denoted by $\sigma_r,\ r = 1, ..., 2^g - 2$, and all odd spin structures would be included in the set $R_0 \cup \cup_r \sigma_r(R_0)$.

With an appropriate definition of the action of σ_r on the remaining odd spin structures, the set $\{\mathbf{1}, \sigma_r\}$ can be mapped isomorphically onto the multiplicative group G_g of nonzero elements of a finite field $(\mathbb{Z}_{2^g-1}, \cdot, +)$ when $2^g - 1$ is prime. As the order of G_g is $|G_g| = 2^g - 1$, the group does not have any proper subgroups. Therefore, in the computation of the odd spin structure part of a superstring amplitude at genus g with $2^g - 1$ being prime, it is not possible to restrict the sum over spin structures to specified sectors while maintaining the invariances of the theory. Modular invariance, in particular, requires a sum over the spin structures which leads to a cancellation of the divergences.

Let $\bar{\Gamma}(1) = PSL(2;\mathbb{Z})$, $\bar{\Gamma}(n)$ be the inhomogeneous congruence subgroup of level n, with the entries of the 2×2 matrix satisfying $ad - bc \equiv 1\ (mod\ n)$ and $\bar{G}(n) = \bar{\Gamma}(1)/\bar{\Gamma}(n)$ [3]. It can be mapped isomorphically to the group of modular transformations acting on one handle factored by the equivalence relation of conjugacy to the same element in the group $\{\mathbf{1}, \sigma_r\}$. The elements of $\bar{G}(p)$ can be divided into $p+1$, $\frac{1}{2}p(p+1)$ and $\frac{1}{2}p(p-1)$ conjugate cyclic groups of order p, $\frac{1}{2}(p-1)$ and $\frac{1}{2}(p+1)$. While the cyclic groups of order p are conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, the other cyclic groups are conjugates of the subgroup generated by $\begin{pmatrix} x & x+1 \\ x-1 & x \end{pmatrix}$ with x being a solution to the congruence relation $F_{\frac{1}{2}(p-1)}(x) \equiv 0\ (mod\ p)$ or $F_{\frac{1}{2}(p+1)}(x) \equiv 0\ (mod\ p)$ [3], where $F_n(x)$ is the defined by $\frac{sinh\ n\theta}{sinh\ \theta}$, $x = cosh\ \theta$, and $F_{n+1}(x)$ is a Chebyshev polynomial of the second kind [13]. If $2^g - 1$ is prime, one solution to $F_{\frac{1}{2}(p+1)} = F_{2^{g-1}}(x) \equiv 0\ (mod\ 2^g - 1)$ is $x = 2$.

The Chebyshev polynomial of the first kind, defined by $T_n(x) = cosh\ n\theta$, $x = cosh\ \theta$ satisfies $T_m(T_n(x)) = T_{mn}(x)$, and

$$T_{2^g}(x) = 2(2T_{2^{g-2}}(x)^2 - 1)^2 - 1 \tag{4.5}$$

For Mersenne primes [17],

$$T_{2^g}(x) - 1 \;\equiv\; (x^2-1)((x^2-1)^{2^{g-1}-1}+1) \quad (mod\ 2^g-1) \tag{4.6}$$

From the relation $T_{\frac{1}{2}(p+1)}(2) = T_{2^{g-1}}(2) \equiv -T_0(2) = -1\ (mod\ 2^g-1)$, it follows that $T_{2^{g-2}}(2) \equiv 0\ (mod\ 2^g-1)$. The congruence condition for a Mersenne prime is then

$$3^{2^{n-1}-1} \;+\; 1 \;\equiv\; 0 \;\; (mod\ 2^n-1) \tag{4.7}$$

It can be shown that $x = T_j(2),\ j\ odd$ also satisfies $T_{2^{g-2}}(x) \equiv 0\ (mod\ 2^g-1)$, so that, for example, when $x = T_3(2) = 26$, the congruence relation is

$$675^{2^{n-1}-1} \;+\; 1 \;\equiv\; 0 \;\; (mod\ 2^n-1) \tag{4.8}$$

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

Let $p \equiv 3\ (mod\ 4)$ be a Mersenne prime index [21] so that

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \;+\; \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \equiv 0 \qquad (mod\ p) \tag{5.1}$$

or equivalently

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} = K_1 p \tag{5.2}$$

for some K_1. The congruence

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} \equiv 0\ (mod\ p') \tag{5.3}$$

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

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} \;=\; \sum_{n=1}^{\bar{N}} K_{2n} p'^n \tag{5.4}$$

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,

$$\begin{aligned} \sum_{n=1}^{\bar{N}} K_{2n} p'^n - K_1 p = \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} &+ \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p'+1}{2}} - \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \\ &- \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \\ = \; f(p') & \end{aligned} \tag{5.5}$$

Suppose for arbitrarily large p' that the function

$$f(x) \;=\; \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{x+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{x+1}{2}} - \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} > 0 \quad (5.6)$$

can be approximated by a polynomial of degree N

$$a_N x^N + ... + a_1 x + a_0 \quad (5.7)$$

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

$$K_{2\bar{N}} p'^{\bar{N}} + ... + K_{21} p' \;=\; f(p') + K_1 p \quad (5.8)$$

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

$$a_0 + K_1 p \equiv 0 \; (mod \; p') \quad (5.9)$$

is required. The constant term can 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

$$\begin{aligned} L(x) \;&=\; \sum_{n=0}^{N} I_n(x) f(x_n) \\ I_n(x) \;&=\; \frac{P(x)}{(x - x_n) P'(x_n)} \\ P(x) \;&=\; \prod_{n=0}^{N} (x - x_n) \end{aligned} \quad (5.10)$$

For the function

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{x+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{x+1}{2}} - \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \quad (5.10)$$

the Lagrangian interpolation would be

$$\begin{aligned} L(x) = \sum_n \prod_{n \neq m} \frac{x - x_m}{x_n - x_m} \Bigg[&\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{x+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{x+1}{2}} \\ &- \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} - \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \Bigg] \end{aligned} \quad (5.11)$$

The congruence condition is now

$$\sum_n \prod_{n\neq m} \frac{x-x_m}{x_n-x_m}\Bigg[\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{x+1}{2}}+\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{x+1}{2}} - \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}}-\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}}\Bigg]+K_1 p\equiv 0 \qquad (mod\ p') \tag{5.12}$$

Given the congruence relation for p' to be a Mersenne prime index, Eq. (5.12) implies

$$\left[1-\sum_n \prod_{n\neq m} \frac{(p'-x_m)}{(x_n-x_m)}\right] K_1 p\equiv 0 \qquad (mod\ p') \tag{5.13}$$

when $\sum_n \frac{(p'-x_m)}{(x_n-x_m)}p$ is an integer. Howver, 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'.

6. Proof the Existence of an Infinite Number of 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, $gcd(a,n)=1$ and $g(n)$ is an integer defined by $f(n)=(n-1)g(n)+f(1)$. If $f(n)$ is an 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,

$$f(n)=f(1)+(n-1)\left(f'(1)+\frac{1}{2!}f''(1)(n-1)+\frac{1}{3!}f'''(1)(n-1)^2+...\right) \tag{6.1}$$

and $g(n)$ is integer since

$$\frac{1}{\ell!}f^{(\ell)}(1)\ =\ \sum_{k\geq 0}\ \frac{1}{\ell!}a_k(k+\ell)(k+\ell-1)...(k+1) \tag{6.2}$$

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

$$a^{f(n)}-b^{f(n)}\equiv a^{f(1)+(n-1)g(n)+Kn}-b^{f(1)+(n-1)g(n)+Kn}\equiv a^{f(1)+K}-b^{f(1)+K} \qquad (mod\ n) \tag{6.3}$$

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 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 if $f(r)$ is a polynomial with integer coefficients [14][15]. Thus, there must be an infinite number of primes such that

$$a^{f(p)} - b^{f(p)} \not\equiv 0 \qquad (mod\ p) \tag{6.4}$$

for any function $f(r)$ which does not have a zero at $r = 1$. Indeed, $a^{f(p)} - b^{f(p)} \neq 0 \qquad (mod\ p)$ for all primes $p > N_0$, given some function $f(r)$, with the exception of $a^{f(p)} - b^{f(p)}$ if it is prime. Choosing functions $f_\ell,\ \ell = 1, 2, 3, ...$ such that $f_i(p_i) = f_j(p_j)$ it follows that

$$a^{f_\ell(p_\ell)} - b^{f_\ell(p_\ell)} \not\equiv 0 \qquad (mod\ p_\ell) \tag{6.5}$$

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 functions f_ℓ can 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 bound 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 arbitrarily large set of primes to a subset of the arguments at which an irreducible integer-valued polynomial is prime, which can be achieved through a Lagrangian interpolation. 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 the number of prime values of $x^k + t$, $k \geq 2$ is greater than any given finite lower bound [9][20]. 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 $\tilde{f}(p_\nu) = f(h(p_\nu)) = f(x_\nu) = p'_\nu$, also has rational coefficients $c_k = \sum_{j=0}^{k} a_k b_{k-j}$ 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 that $f_i(p_i) = f_\ell(p_\ell)$ and $\{p_1, p_2, ...\}$ represents the entire set of primes. It follows that $f_1 = f \circ h_1 : \{2, 3, 5, ...\} \rightarrow \{p'_1, p'_2, p'_3, ...\}$, $f_2 = f \circ h_2 : \{3, 5, 7, ...\} \rightarrow \{p'_1, p'_2, p'_3, ...\}$, $f_3 = f_\circ h_3 : \{5, 7, 11, ...\} to \{p'_1, p'_2, p'_3, ...\}$, ... The range of values of the exponent for which $a^t - b^t \not\equiv 0 \quad (mod\ p)$, $p > sup_\ell N_\ell$, is given by $\cap_{\substack{\ell,p \\ p>supN_\ell}} f_\ell(p) = \cap_\ell\ f_\ell(p)$ since the functions must satisfy $f_i(p_i) = f_j(p_j)$. It is 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 $\{f'_\wp\}$ would shift the value of $sup_\ell\ N_\ell$ to $sup_\wp\ N'_\wp$, and it would not be necessarily possible to bound the prime divisors of $a^{F(p)} - b^{F(p)}$, $\{F\} = \{f_\ell, f'_\wp, ...\}$.

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 prime 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 $2kq + 1 \leq sup_\ell\ N_\ell$. The functions $\{f_\ell\}$ can be chosen such that $2^{f_\ell(1)+K_\ell}$ does not have prime divisors greater than $2q + 1$. Thus, if $q > \frac{sup_\ell\ N_\ell - 1}{2}$ can be identified with $f_\ell(p_\ell)$ for some value of p_ℓ and for all ℓ, $2^q - 1 \not\equiv 0\ (mod\ p)$ for all primes p except for $2^q - 1$. When $a \neq b + 1$, the factorization of $a^n - b^n$ for all $n \in \mathbb{Z},\ n \geq 2$, 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 $2^q - 1 \neq 0\ (mod\ n)$ for all $n > 1,\ n \neq 2^q - 1$, the only integer divisors of $2^q - 1$ are 1 and $2^q - 1$, so that $2^q - 1$ is prime. It follows that the set of primes exponents q such that $2^q - 1$ is prime is arbitrarily large. By induction, the infinite extent of the sequence of Mersenne primes is then proven.

Acknowledgements

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

References

[1] M. Atiyah, Ann. Scient. Ecole Norm. Sup. V **4** (1971) 47-62

[2] A. S. Bang, Taltheoretische Undersogseler. Tidsskrift for Mathematik. **5** 70-80; 130-137 (1886)

[3] T. Bang, Congruence Properties of Tchebycheff Polynomials, *Math. Scand.* 2 (1954) 327-333

[4] G. D. Birkhoff and H. S. Vandiver, On the Integral Divisors of $a^n - b^n$. Ann. Math. **5** 173-180 (1904)

[5] V. Chothi, G. Everest and T. Ward, S-Integer Dynamical Systems: Periodic Points, *J. Reine Angew. Math.* **489** (1997) 99-132

[6] G. S. Danilov, *Nucl. Phys.* **B463** (1996) 443

[7] 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

[8] S. Davis, A Recurrence Relation for the Number of Goldbach Partitions of an Even Integer, RFSC/04/06

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

[10] D. Johnson, it J. London Math. Soc. **22** (1980) 365-373

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

[12] E.Lucas, Theorie des Fonctions Numeriques Simplement Pŕiodiques. Amer. J. Math. **1** 289-321 (1878)

[13] W. Magnus, F. Oberhettinger and R. P. Soni, *Formulas and Theorems for the Special Functions of Mathematical Physics* (Springer-Verlag: New York, 1966)

[14] 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. 3 141-147 (1987)

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

[16] W. Narkiewicz, The Development of Prime Number Theory. (Springer-Verlag, 2000)

[17] R. A. Rankin, Chebyshev Polynomials and the Modular Group of Level p, *Math. Scand.* **2** (1954) 315-326

[18] B. de la Rosa, Fibonacci Quart. **16**(6) 518-522 (1978)

[19] M. du Sautoy, Mersenne Primes, Irrationality and Counting Subgroups, *Bull. Lond. Math. Soc.* **29** (1997) 285-294

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

[21] W. Sierpinski, *Elementary Theory of Numbers* Mongrafie Matematyczyne Tom 42 (Warszawa: Pańtwowe Wydawnictwo Naukowe, 1964)

[22] A. G. Wolman, *J. Reine Angew. Math.* **477** (1996) 31-70

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

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