symmetry

Article

Global Generalized Mersenne Numbers: Definition, Decomposition, and Generalized Theorems

Vladimir Pletser [1,2,†]

[1] European Space Research and Technology Centre, European Space Agency, 2201 AZ Noordwijk, The Netherlands
[2] Blue Abyss, Pool Innovation Centre, Newquay TR15 3PL, UK; vladimir.pletser@blueabyss.uk
[†] Retired from European Space Agency.

Abstract: A new generalized definition of Mersenne numbers is proposed of the form $(a^n - (a-1)^n)$, called global generalized Mersenne numbers and noted $GM_{a,n}$ with base a and exponent n positive integers. The properties are investigated for prime n and several theorems on Mersenne numbers regarding their congruence properties are generalized and demonstrated. It is found that for any a, $(GM_{a,n} - 1)$ is even and divisible by n, a and $(a-1)$ for any prime $n > 2$, and by $(a(a-1)+1)$ for any prime $n > 5$. The remaining factor is a function of triangular numbers of $(a-1)$, specific for each prime n. Four theorems on Mersenne numbers are generalized and four new theorems are demonstrated, showing first that $GM_{a,n} \equiv (1 \text{ or } 7)(\text{mod } 12)$ depending on the congruence of $a(\text{mod } 4)$; second, that $(GM_{a,n} - 1)$ are divisible by 10 if $n \equiv 1(\text{mod } 4)$ and, if $n \equiv 3(\text{mod } 4)$, $GM_{a,n} \equiv (1 \text{ or } 7 \text{ or } 9)(\text{mod } 10)$, depending on the congruence of $a(\text{mod } 5)$; third, that all factors c_i of $GM_{a,n}$ are of the form $(2nf_i + 1)$ such that c_i is either prime or the product of primes of the form $(2nj + 1)$, with f_i, j natural integers; fourth, that for prime $n > 2$, all $GM_{a,n}$ are periodically congruent to $(\pm 1 \text{ or } \pm 3)(\text{mod } 8)$ depending on the congruence of $a(\text{mod } 8)$; and fifth, that the factors of a composite $GM_{a,n}$ are of the form $(2nf_i + 1)$ with $f_i \equiv u(\text{mod } 4)$ with $u = 0, 1, 2$ or 3 depending on the congruences of $n(\text{mod } 4)$ and of $a(\text{mod } 8)$. The potential use of generalized Mersenne primes in cryptography is shortly addressed.

Keywords: Mersenne numbers; generalized Mersenne numbers; divisibility and congruence properties

MSC: 11A07; 11A67; 11Y05; 11Y55

Citation: Pletser, V. Global Generalized Mersenne Numbers: Definition, Decomposition, and Generalized Theorems. *Symmetry* **2024**, *16*, 551. https://doi.org/10.3390/sym16050551

Academic Editors: Sergei D. Odintsov and Calogero Vetro

Received: 8 February 2024
Revised: 16 April 2024
Accepted: 18 April 2024
Published: 3 May 2024

1. Introduction

It is known that if a Mersenne number of the form $M_n = (2^n - 1)$ is prime, then n is prime. The reciprocal is not true, as, for example, for $n = 11$, M_{11} is composite, $M_{11} = 2047 = 23 \cdot 89$ (for review, see, e.g., [1–3]). There are 51 Mersenne prime numbers known [4]. The largest appears for $n = 82589933$, $M_{82589933} = (2_{82589933} - 1)$, and has 24862048 digits.

Due to their intensive use in cryptography, several generalizations of Mersenne numbers have been proposed, first by Crandall [5] of the form $(2^n - C)$ where C is a small odd natural integer number; then by Solinas [6–8] of the form $(2^n + \epsilon_3 2^{m_3} + \epsilon_2 2^{m_2} + \epsilon_1 2^{m_1} + \epsilon_0)$ which generalized also Fermat numbers and where $\epsilon_i = -1, 0$ or $+1$, m_i and n are multiple of s, the length of a computer word (e.g., $s = 32$); and finally, further generalized [9] in the form $\left(2^n + \sum_{i=1}^{k} [\epsilon_i 2^{m_i}] + \epsilon_0\right)$ with n, k and m_i being natural integers, $1 \leq k < n$, $1 \leq m_i < n$ and $\epsilon_i = -1, 0$ or $+1$. Hoque and Saikia proposed [10,11] another definition of generalized Mersenne numbers as $M_{p,q} = (p^q - p + 1)$, where p, q are positive integers. Deng introduced [12] a different definition of generalized Mersenne primes, which is of the form $R(k, p) = (p^k - 1)/(p - 1)$, where k, p and $R(k, p)$ are prime numbers.

We propose here another generalized definition of Mersenne numbers of the form $(a^n - (a-1)^n)$ with a and n natural integers. Although the name generalized Mersenne number is already in use for pseudo-Mersenne numbers of the form proposed by Crandall [5], Solinas [6–8], and others, we propose to call them global generalized Mersenne numbers, or in short, generalized Mersenne ($GM_{a,n}$) numbers (see also [13]), referring to the fact that both the base a and the exponent n can take any integer values > 1.

This new generalization of Mersenne numbers is unrelated to previous ones as there are major differences in the form, the bases a and the exponents n (with the notations of this paper). The generalization of Crandall considers a fixed base 2 and a small odd natural integer as the second term; the generalization of Solinas has also a fixed base 2 and a multiple algebraic sum with only composite exponents n. The generalization of Hoque and Saikia has a variable base p and a similar second term $(p-1)$, but without exponentiation. The generalization proposed by Deng is even more different, with a prime base p and a form as a polynomial in p of degree $(k-1)$.

In this paper, we explore the properties of global generalized Mersenne numbers, and more specifically those $GM_{a,n}$ obtained for prime exponents n. Generalized Mersenne numbers are defined in Section 2.1. Section 2.2 gives several decompositions of $GM_{a,n}$. Several theorems on congruence of Mersenne numbers are generalized for $GM_{a,n}$ in Section 2.3. Congruence properties of $GM_{a,n}$ and of their factors are investigated in Section 2.4. The density of Mersenne primes and the potential use of generalized Mersenne primes in cryptography are shortly discussed in Section 3. Conclusions are drawn in Section 4.

2. Materials and Methods

2.1. Global Generalized Mersenne Numbers

Mersenne numbers can be seen as the difference of the nth power of the first two successive integers

$$M_n = (2^n - 1) = (2^n - 1^n). \tag{1}$$

By extension, global generalized Mersenne (GM) numbers, noted $GM_{a,n}$, are defined as the difference of the nth power of two successive integers

$$GM_{a,n} = (a^n - (a-1)^n) \tag{2}$$

and indexed by the base a and the exponent n, with $a \geq 2$ and $n \geq 2$ natural integers.

It is easy to show, like for Mersenne numbers, that generalized Mersenne numbers can only be primes if n itself is prime. Indeed, if n is composite, $n = rs$ with r and s natural positive integers, then all $GM_{a,n} = (a^{rs} - (a-1)^{rs})$ are binomial numbers, having $(a^r - (a-1)^r)$ or $(a^s - (a-1)^s)$ as integer factor. Therefore, in the rest of this paper, we will consider only the cases of n being prime as we want to investigate the properties of generalized Mersenne primes.

Table 1 shows the first 25 $GM_{a,n}$ numbers for the first five primes $n = 2, 3, 5, 7, 11$, with $GM_{a,n}$ prime and composite numbers shown, respectively, in bold and italic characters.

For $n = 2$, (2) yields all the odd integers $GM_{a,2} = 2a - 1$. For $n = 3$, the first four $GM_{a,3}$ numbers are prime for $a = 2$ to 5; further numbers are composite or prime without any seemingly regular pattern. For $n = 5$ and 7 and $a = 2$, $GM_{2,5}$ and $GM_{2,7}$ are the Mersenne primes M_5 and M_7. For $3 \leq a \leq 19$, interesting patterns occur in the two $GM_{a,5}$ and $GM_{a,7}$ series. For $a = 3$ and 4, $GM_{a,5}$ and $GM_{a,7}$ are oppositely prime and composite. For $a = 5$, $GM_{a,5}$ and $GM_{a,7}$ are both composites. For $a = 6$ to 12, $GM_{a,5}$ and $GM_{a,7}$ are oppositely primes and composites again, with a series of composite $GM_{a,5}$ and prime $GM_{a,7}$ for $a = 7$ to 10. For $a = 13$ to 19, $GM_{a,5}$ and $GM_{a,7}$ are composites or primes for same values of a. For larger values of a, regular patterns between $GM_{a,5}$ and $GM_{a,7}$ disappear and reappear for certain ranges of values of a. For $n = 11$, the first four $GM_{a,11}$ are composite (the fifth Mersenne number $M_{11} = 2047$ is not prime). Among the first 25 $GM_{a,11}$, the values for $a = 6, 8, 10$ and 14 yield prime numbers.

It is observed that for odd values of n with $n \equiv 1 (\bmod 4)$, the series of $GM_{a,n}$ numbers generated for successive values of the base a have 1 as the last digit, while for odd values of n with $n \equiv 3 (\bmod 4)$, the series of the last digit of $GM_{a,n}$ numbers are repetitions of the sequence $1, 7, 9, 7, 1$, respectively, for bases $a \equiv k (\bmod 5)$, with k, respectively $1, 2, 3, 4, 0$. This is demonstrated further in Section 2.3.3.

Table 1. First 25 $GM_{a,n}$ numbers for $n = 2, 3, 5, 7, 11$.

a	***n* = 2**	***n* = 3**	***n* = 5**	***n* = 7**	***n* = 11**
2	**3**	**7**	**31**	**127**	*2047*
3	**5**	**19**	**211**	*2059*	*175099*
4	**7**	**37**	*781*	**14197**	*4017157*
5	*9*	**61**	*2101*	*61741*	*44633821*
6	**11**	*91*	**4651**	*201811*	**313968931**
7	**13**	**127**	*9031*	**543607**	*1614529687*
8	*15*	*169*	*15961*	**1273609**	**6612607849**
9	**17**	*217*	*26281*	**2685817**	*22791125017*
10	**19**	**271**	*40951*	**5217031**	**68618940391**
11	*21*	**331**	**61051**	*9487171*	*185311670611*
12	**23**	**397**	*87781*	**16344637**	*457696700077*
13	*25*	*469*	*122461*	*26916709*	*1049152023349*
14	*27*	**547**	*166531*	*42664987*	*2257404775627*
15	**29**	**631**	*221551*	*65445871*	*4600190689711*
16	**31**	*721*	*289201*	*97576081*	*8942430185041*
17	*33*	*817*	**371281**	**141903217**	*16679710263217*
18	*35*	**919**	*469711*	*201881359*	*29996513771599*
19	**37**	*1027*	*586531*	*281651707*	*52221848818987*
20	*39*	*1141*	**723901**	*386128261*	*88309741101781*
21	**41**	*1261*	*884101*	*521088541*	*145477500542221*
22	**43**	*1387*	*1069531*	*693269347*	*234040800869107*
23	*45*	*1519*	*1282711*	*910467559*	*368491456502599*
24	**47**	**1657**	*1526281*	*1181645977*	*568871385255097*
25	49	**1801**	**1803001**	*1517044201*	*862504647846601*

The cause of these patterns, or lack of it, in the distributions of composite and prime generalized Mersenne numbers is tantalizing. The beginning of an answer is given in the next sections.

2.2. Decomposition of Generalized Mersenne Numbers

It is known that all Mersenne numbers and their factors can be written in the form

$$M_n = 2nq + 1 \tag{3}$$

with q and n positive natural integer and n prime (see e.g., [1,14,15]). All generalized Mersenne numbers can also be written in a similar form as demonstrated in the following theorem.

Theorem 1. *For a and n natural integers, $n > 2$, all generalized Mersenne numbers can be written as*

$$GM_{a,n} = 2nQ_n(a) + 1 \tag{4}$$

for all prime exponents $n > 2$ and for all bases a, and where $Q_n(a)$ is a polynomial in a of degree $n-1$.

Proof. Let a and n be natural integers, n prime, $n > 2$. Applying Fermat's little theorem to a^n and to $(a-1)^n$ yields immediately that $GM_{a,n} \equiv 1(\bmod n)$ and, as all $GM_{a,n}$ (2) are always odd as the difference of the powers of consecutive integers a and $(a-1)$ is always odd, then $GM_{a,n} \equiv 1(\bmod 2n)$. Therefore, the polynomial $Q_n(a)$ takes integer values for integral a. To find the expression of this polynomial and to show that its degree is $n-1$, (2) is developed as follows. Posing

$$d_i^n = \frac{\binom{n}{i}}{n} = \frac{(n-1)!}{i!(n-i)!} \tag{5}$$

with $\binom{n}{i}$ the binomial coefficient, writing $\triangle$ for convenience for the triangular number of $(a-1)$, $\triangle = \triangle(a-1) = \frac{a(a-1)}{2}$, and noting that the exponent n is odd, developing (2) yields successively

$$\begin{aligned}
GM_{a,n} &= \left(a^n - \left(a^n + \sum_{i=1}^{n-1}\left[(-1)^i\binom{n}{i}a^{n-i}\right] - 1\right)\right) = \sum_{i=1}^{n-1}\left[(-1)^{i+1}\binom{n}{i}a^{n-i}\right] + 1 \\
&= n\sum_{i=1}^{n-1}\left[(-1)^{i+1}d_i^n a^{n-i}\right] + 1 = n\sum_{i=1}^{\frac{n-1}{2}}\left[(-1)^{i+1}d_i^n\left(a^{n-i} - a^i\right)\right] + 1 \\
&= n\sum_{i=1}^{\frac{n-1}{2}}\left[(-1)^{i+1}d_i^n a^i\left(a^{n-2i} - 1\right)\right] + 1 \\
&= n\sum_{i=1}^{\frac{n-1}{2}}\left[(-1)^{i+1}d_i^n a^i(a-1)\sum_{j=0}^{n-1-2i}\left[a^{n-1-2i-j}\right]\right] + 1 \\
&= na(a-1)\sum_{i=1}^{\frac{n-1}{2}}\left[(-1)^{i+1}d_i^n\sum_{j=0}^{n-1-2i}\left[a^{n-2-i-j}\right]\right] + 1 \\
&= 2n\triangle\sum_{i=1}^{n-2}\left[S_i^{(1)}a^{n-2-i}\right] + 1
\end{aligned} \tag{6}$$

where, for $1 \leq i \leq \frac{n-1}{2}$,

$$S_i^{(1)} = \sum_{j=1}^{i}\left[(-1)^{j+1}d_j^n\right] \tag{7}$$

and for $\frac{n+1}{2} \leq i \leq n-2$,

$$S_i^{(1)} = \sum_{j=i+1}^{n-1}\left[(-1)^j d_j^n\right] = S_{n-1-i}^{(1)}. \tag{8}$$

Relation (6) shows that the positive integer function $Q_n(a)$ depends only on the variable a and is a polynomial in a of degree $n-1$. □

Note that the polynomial $Q_n(a)$ does not have integer coefficients as the triangular number $\triangle = \frac{a(a-1)}{2}$ is a factor in front of the polynomial. However, the polynomial $Q_n(a)$ takes integer values for all integers a. Note also that d_i^n(5) always take integer values, as shown by Ram [16] (see also [17]).

One can characterize further the polynomial $Q_n(a)$ for higher values of n in Theorem 2.

Theorem 2. *For a and n natural integers, $n > 2$, all generalized Mersenne numbers can be written as*

$$GM_{a,n} = 2n\left(\triangle Q'_n(2\triangle)\right) + 1 \tag{9}$$

for all prime exponents $n \geq 3$, and as

$$GM_{a,n} = 2n\left(\triangle(2\triangle + 1)Q''_n(2\triangle)\right) + 1 \tag{10}$$

for all prime exponents $n \geq 5$ and for all bases a, where $Q'_n(2\triangle)$ and $Q''_n(2\Delta)$ are polynomials in the variable $\triangle(a-1)$ only, the triangular number of $(a-1)$, and of degrees $\left(\frac{n-3}{2}\right)$ and $\left(\frac{n-5}{2}\right)$, respectively.

Proof. Let a, n, i, j, J, k be natural integers, with n prime, $n > 2$ and $i < n$.

We show first that $GM_{a,n}$ is a polynomial in $\triangle(a-1)$.

$$\begin{aligned}
GM_{a,n} &= a^n - (a-1)^n \\
&= \left(\frac{1}{2} + \left(a - \frac{1}{2}\right)\right)^n + \left(\frac{1}{2} - \left(a - \frac{1}{2}\right)\right)^n \\
&= 2\sum_{k=0}^{(n-1)/2} \binom{n}{2k} \left(\frac{1}{2}\right)^{n-2k} \left(a - \frac{1}{2}\right)^{2k} \text{(the odd terms cancel)} \\
&= 2\sum_{k=0}^{(n-1)/2} \binom{n}{2k} \left(\frac{1}{2}\right)^{n-2k} \left(a^2 - a + \frac{1}{4}\right)^{k}
\end{aligned} \tag{11}$$

which is clearly a polynomial in $\triangle = \frac{a^2-a}{2}$.

We show now that $Q'_n(2\triangle)$ and $Q''_n(2\Delta)$ are polynomials of degrees $\left(\frac{n-3}{2}\right)$ and $\left(\frac{n-5}{2}\right)$, respectively. Continuing from (6) the development of the polynomial (2) in $\frac{(n-1)}{2}$ successive iterations, one obtains an expression of $GM_{a,n}$ as a polynomial of degree $\frac{(n-1)}{2}$ in $\triangle$ in the form

$$GM_{a,n} = 2n\triangle\left(\sum_{i=0}^{\frac{n-3}{2}}\left[(2\triangle)^i S_{n-2(i+1)}^{(i+1)}\right]\right) + 1 = 2n\triangle\left(\sum_{i=0}^{\frac{n-3}{2}}\left[(2\triangle)^i \frac{\binom{n-i-2}{i}}{i+1}\right]\right) + 1. \tag{12}$$

The polynomial $Q_n(a)$ in (4) can be deduced as a function of $\triangle$ from (12)

$$Q_n(a) = \triangle\left(\sum_{i=0}^{\frac{n-3}{2}}\left[(2\triangle)^i S_{n-2(i+1)}^{(i+1)}\right]\right). \tag{13}$$

The polynomial $Q'_n(2\triangle)$ in (9) can be deduced from (13)

$$Q'_n(2\triangle) = \sum_{k=1}^{\frac{n-1}{2}}\left[(2\triangle)^{k-1} S_{n-2k}^{(k)}\right] = \sum_{k=1}^{\frac{n-1}{2}}\left[(2\triangle)^{k-1} \frac{\binom{n-k-1}{k-1}}{k}\right]. \tag{14}$$

For $n \geq 5$, factoring the right side of (12) by $(2\triangle + 1)$ yields $GM_{a,n} = 2n\triangle(2\triangle + 1)Q''_n(2\triangle) + 1$, with the polynomial $Q''_n(2\triangle)$

$$Q''_n(2\triangle) = \sum_{i=0}^{\frac{n-5}{2}}\left[(2\triangle)^i \sum_{j=0}^{\frac{n-5}{2}-i}\left[(-1)^{\frac{n-5}{2}-i+j} S_{2j+1}^{\left(\frac{n-1}{2}-j\right)}\right]\right] \tag{15}$$

or inversely, by inverting the sums,

$$Q''_n(2\triangle) = (-1)^{\frac{n-5}{2}} \sum_{j=0}^{\frac{n-5}{2}} \left[(-1)^j S_{2j+1}^{\left(\frac{n-1}{2}-j\right)} \sum_{i=0}^{\frac{n-5}{2}-j} \left[(-2\triangle)^i \right] \right] \tag{16}$$

and where

$$S_{2j+1}^{\left(\frac{n-1}{2}-j\right)} = \frac{\binom{\frac{n-1}{2}+j}{2j}}{(2j+1)}. \tag{17}$$

Therefore, the general form of all $GM_{a,n}$ can be written as in (9) and (10) for n prime, respectively $n \geq 3$ and $n \geq 5$, where the polynomials $Q'_n(2\triangle)$ and $Q''_n(2\triangle)$ of the variable $\triangle(a-1)$ have degrees, respectively $\left(\frac{n-3}{2}\right)$ and $\left(\frac{n-5}{2}\right)$. $\square$

Note that polynomials $Q'_n(2\triangle)$ and $Q''_n(2\triangle)$ take integer values as coefficients $S_{n-2k}^{(k)} = \frac{\binom{n-k-1}{k-1}}{k}$ in (12), and $S_{2j+1}^{\left(\frac{n-1}{2}-j\right)} = \frac{\binom{\frac{n-1}{2}+j}{2j}}{(2j+1)}$ in (17) are always integers, as shown by Catalan [18] (see also [17]).

Note furthermore that for large values of the exponent n, the calculation of $GM_{a,n}$ becomes quickly intractable as nth powers become difficult to compute. The development given in Theorem 2 for odd prime values of n gives an alternate method to calculate $GM_{a,n}$ by reducing the degree of the polynomial (2) from n to $\left(\frac{n-1}{2}\right)$, and by using the new variable $\triangle(a-1)$, the triangular number of $(a-1)$, instead of the variable a.

For very large values of a and n, the value of a $GM_{a,n}$ is dominated by the first term in the polynomial (12), and can therefore be approximated by

$$GM_{a,n} \approx na^{n-1} \tag{18}$$

for $a \gg 1$ and n prime $\gg 1$, with the approximation growing better for increasingly larger values of a and n, and even better for $a \gg n$.

For the first six odd prime values of the exponent n, the polynomial expression of $GM_{a,n}$ gives, with further factorization,

$$GM_{a,3} = 2 \cdot 3\triangle + 1 \tag{19}$$

$$GM_{a,5} = 2 \cdot 5\triangle(2\triangle + 1) + 1 \tag{20}$$

$$GM_{a,7} = 2 \cdot 7\triangle(2\triangle + 1)^2 + 1 \tag{21}$$

$$GM_{a,11} = 2 \cdot 11\triangle(2\triangle + 1)[2\triangle(2\triangle + 1)(2\triangle + 3) + 1] + 1 \tag{22}$$

$$GM_{a,13} = 2 \cdot 13\triangle(2\triangle + 1)^2\{(2\triangle + 1)[(2\triangle + 1)(2\triangle + 3) - 4] + 2\} + 1 \tag{23}$$

$$GM_{a,17} = 2 \cdot 17\triangle(2\triangle + 1)\{(2\triangle + 1)[(2\triangle + 1)((2\triangle + 1)\{(2\triangle + 1)\ ]\ [(2\triangle + 1)(2\triangle + 6) - 9] + 1\} + 6) - 4] + 1\} + 1 \tag{24}$$

etc., where, to recall, $\triangle$ is written for $\triangle(a-1)$ and where several factorizations are possible for $n \geq 13$. As a further example, Table 2 show the first ten values of $GM_{a,n}$ for prime exponents n from 3 to 11, with the decomposition (19)–(22) in integer factors of $(GM_{a,n} - 1)$.

Table 2. Decomposition of generalized Mersenne numbers $GM_{a,n}$ for $2 \leq a \leq 10$.

$\boldsymbol{GM_{a,3}}$	$\boldsymbol{= 2 \cdot 3 \cdot \triangle + 1}$	**Decomposition of** $\boldsymbol{(GM_{a,3} - 1)}$
7	$2 \cdot 3 \cdot 1 + 1$	prime
19	$2 \cdot 3 \cdot 3 + 1$	prime
37	$2 \cdot 3 \cdot 6 + 1$	prime
61	$2 \cdot 3 \cdot 10 + 1$	prime
91	$2 \cdot 3 \cdot 15 + 1$	$7 \cdot 13 = (2 \cdot 3 + 1)(2^2 \cdot 3 + 1)$
127	$2 \cdot 3 \cdot 21 + 1$	prime
169	$2 \cdot 3 \cdot 28 + 1$	$13^2 = (2^2 \cdot 3 + 1)^2$
217	$2 \cdot 3 \cdot 36 + 1$	$7 \cdot 31 = (2 \cdot 3 + 1)(2 \cdot 3 \cdot 5 + 1)$
271	$2 \cdot 3 \cdot 45 + 1$	prime
$\boldsymbol{GM_{a,5}}$	$\boldsymbol{2 \cdot 5 \cdot \triangle \cdot (2\triangle + 1) + 1}$	**Decomposition of** $\boldsymbol{(GM_{a,5} - 1)}$
31	$2 \cdot 5 \cdot 1 \cdot 3 + 1$	prime
211	$2 \cdot 5 \cdot 3 \cdot 7 + 1$	prime
781	$2 \cdot 5 \cdot 6 \cdot 13 + 1$	$11 \cdot 71 = (2 \cdot 5 + 1)(2 \cdot 5 \cdot 7 + 1)$
2101	$2 \cdot 5 \cdot 10 \cdot 21 + 1$	$11 \cdot 191 = (2 \cdot 5 + 1)(2 \cdot 5 \cdot 19 + 1)$
4651	$2 \cdot 5 \cdot 15 \cdot 31 + 1$	prime
9031	$2 \cdot 5 \cdot 21 \cdot 43 + 1$	$11 \cdot 821 = (2 \cdot 5 + 1)(2^2 \cdot 5 \cdot 41 + 1)$
15961	$2 \cdot 5 \cdot 28 \cdot 57 + 1$	$11 \cdot 1451 = (2 \cdot 5 + 1)(2 \cdot 5^2 \cdot 29 + 1)$
26281	$2 \cdot 5 \cdot 36 \cdot 73 + 1$	$41 \cdot 641 = (2^3 \cdot 5 + 1)(2^7 \cdot 5 + 1)$
40951	$2 \cdot 5 \cdot 45 \cdot 91 + 1$	$31 \cdot 1321 = (2 \cdot 5 \cdot 3 + 1)(2^3 \cdot 5 \cdot 3 \cdot 11 + 1)$
$\boldsymbol{GM_{a,7}}$	$\boldsymbol{2 \cdot 7 \cdot \triangle \cdot (2\triangle + 1)^2 + 1}$	**Decomposition of** $\boldsymbol{(GM_{a,7} - 1)}$
127	$2 \cdot 7 \cdot 1 \cdot 3^2 + 1$	prime
2059	$2 \cdot 7 \cdot 3 \cdot 7^2 + 1$	$29 \cdot 71 = (2^2 \cdot 7 + 1)(2 \cdot 7 \cdot 5 + 1)$
14197	$2 \cdot 7 \cdot 6 \cdot 13^2 + 1$	prime
61741	$2 \cdot 7 \cdot 10 \cdot 21^2 + 1$	$29 \cdot 2129 = (2^2 \cdot 7 + 1)(2^4 \cdot 7 * 19 + 1)$
201811	$2 \cdot 7 \cdot 15 \cdot 31^2 + 1$	$29 \cdot 6959 = (2^2 \cdot 7 + 1)(2 \cdot 7^2 * 71 + 1)$
543607	$2 \cdot 7 \cdot 21 \cdot 43^2 + 1$	prime
1273609	$2 \cdot 7 \cdot 28 \cdot 57^2 + 1$	prime
2685817	$2 \cdot 7 \cdot 36 \cdot 73^2 + 1$	prime
5217031	$2 \cdot 7 \cdot 45 \cdot 91^2 + 1$	prime
$\boldsymbol{GM_{a,11}}$	$\boldsymbol{2 \cdot 11\triangle(2\triangle + 1)[2\triangle(2\triangle + 1)(2\triangle + 3) + 1] + 1}$	
2047	$2 \cdot 11 \cdot 1 \cdot 3[2 \cdot 1 \cdot 3 \cdot 5 + 1] + 1$	
175099	$2 \cdot 11 \cdot 3 \cdot 7[2 \cdot 3 \cdot 7 \cdot 9 + 1] + 1$	
4017157	$2 \cdot 11 \cdot 6 \cdot 13[2 \cdot 6 \cdot 13 \cdot 15 + 1] + 1$	
44633821	$2 \cdot 11 \cdot 10 \cdot 21[2 \cdot 10 \cdot 21 \cdot 23 + 1] + 1$	
313968931	$2 \cdot 11 \cdot 15 \cdot 31[2 \cdot 15 \cdot 31 \cdot 33 + 1] + 1$	
1614529687	$2 \cdot 11 \cdot 21 \cdot 43[2 \cdot 21 \cdot 43 \cdot 45 + 1] + 1$	
6612607849	$2 \cdot 11 \cdot 28 \cdot 57[2 \cdot 28 \cdot 57 \cdot 59 + 1] + 1$	
22791125017	$2 \cdot 11 \cdot 36 \cdot 73[2 \cdot 36 \cdot 73 \cdot 75 + 1] + 1$	
68618940391	$2 \cdot 11 \cdot 45 \cdot 91[2 \cdot 45 \cdot 91 \cdot 93 + 1] + 1$	
$\boldsymbol{GM_{a,11}}$	**Decomposition of** $\boldsymbol{(GM_{a,11} - 1)}$	
2047	$23 \cdot 89 = (2 \cdot 11 + 1)(2^3 \cdot 11 + 1)$	
175099	$23^2 \cdot 331 = (2 \cdot 11 + 1)^2(2 \cdot 11 \cdot 3 \cdot 5 + 1)$	
4017157	$23 \cdot 174659 = (2 \cdot 11 + 1)(2 \cdot 11 \cdot 17 \cdot 467 + 1)$	
44633821	$6359 \cdot 7019 = (2 \cdot 11 \cdot 17^2 + 1)(2 \cdot 11^2 \cdot 29 + 1)$	
313968931	prime	
1614529687	$89 \cdot 18140783 = (2^3 \cdot 11 + 1)(2 \cdot 11 \cdot 19 \cdot 43399 + 1)$	
6612607849	prime	
22791125017	$23 \cdot 990918479 = (2 \cdot 11 + 1)(2 \cdot 11 \cdot 45041749 + 1)$	
68618940391	prime	

2.3. Congruence Properties of Generalized Mersenne Numbers

2.3.1. Corollary on Congruence of Generalized Mersenne Numbers

We start first with a corollary of Theorem 2.

Corollary 1. *For all natural integer bases $a \geq 2$, all generalized Mersenne numbers are such that*

$$GM_{a,n} \equiv 1(mod\, 2n) \tag{25}$$
$$GM_{a,n} \equiv 1(mod\, a) \tag{26}$$
$$GM_{a,n} \equiv 1(mod\, (a-1)) \tag{27}$$

for all natural integer prime exponents $n \geq 3$ and

$$GM_{a,n} \equiv 1(mod\, (a(a-1)+1)) \tag{28}$$
$$GM_{a,n} \equiv 1\left(mod\, \left(a(a-1)\left(a^2-a+1\right)\right)\right) \tag{29}$$

for all natural integer prime exponents $n \geq 5$.

Proof. Let a and n be natural integers with $a \geq 2$ and n prime, $n \geq 3$. Relation (25) was already used in the proof of Theorem 1. Relations (26) and (27) are deduced directly from (9); (28) and (29) are deduced from (10) as polynomials $Q'_n(2\triangle)$ and $Q''_n(2\triangle)$ take integer values. □

Note that for $n = 2$, $GM_{a,2} \equiv \pm 1(\mathrm{mod}\, 4)$ obviously as $GM_{a,2}$ are all odd natural integers.

2.3.2. Generalization of a First Theorem on Congruence of Mersenne Numbers

Several theorems are known on the congruence of Mersenne numbers and their factors (see e.g., [1,14]). These can easily be extended to generalized Mersenne numbers.

With notations of this paper, a first theorem on Mersenne numbers states that if n is odd, $n \geq 3$, then $M_n \equiv 7(\mathrm{mod}\, 12)$. This theorem is generalized as follows:

Theorem 3. *For all natural integer bases $a \geq 2$, and for all natural integer prime exponents $n \geq 3$, all generalized Mersenne numbers are such that*

$$GM_{a,n} \equiv 1(mod\, 6) \tag{30}$$

and more precisely,

$$GM_{a,n} \equiv 1(mod\, 12) \quad \text{if } a \equiv 0(mod\, 4) \quad \text{or } 1(mod\, 4) \tag{31}$$
$$GM_{a,n} \equiv 7(mod\, 12) \quad \text{if } a \equiv 2(mod\, 4) \quad \text{or } 3(mod\, 4). \tag{32}$$

Proof. Let a, n, r, α, β be natural integers with $a \geq 2$, $0 \leq \alpha \leq 2$, $0 \leq \beta \leq 3$, and n prime, $n \geq 3$.

(i) Writing $a \equiv \alpha(\mathrm{mod}\, 3)$ and taking the congruence modulo 3 of $GM_{a,n}$ (2) yields $GM_{a,n} \equiv (\alpha^n - (\alpha-1)^n)(\mathrm{mod}\, 3) \equiv 1(\mathrm{mod}\, 3)$ for $\alpha = 0$ to 2. As all $GM_{a,n}$ are odd, all $GM_{a,n}$ must be congruent to 1 modulo 6.

(ii) Writing $a \equiv \beta(\mathrm{mod}\, 4)$ and taking the congruence modulo 4 of $GM_{a,n}$ (2) yields $GM_{a,n} \equiv (\alpha^n - (\alpha-1)^n)(\mathrm{mod}\, 4) \equiv 1(\mathrm{mod}\, 4)$ for $\alpha = 0$ and 1, and $GM_{a,n} \equiv 3(\mathrm{mod}\, 4)$ for $\alpha = 2$ and 3. As all $GM_{a,n}$ are odd and congruent to 1 modulo 6, it yields (31) and (32). □

2.3.3. Theorem on Congruence of Generalized Mersenne Numbers

A new theorem on generalized Mersenne numbers is proposed as follows.

Theorem 4. *For all natural integer bases $a \geq 2$, and for natural integer prime exponents $n \geq 3$, all generalized Mersenne numbers are such that if $n \equiv 1(mod\,4)$,*

$$GM_{a,n} \equiv 1(mod\,10) \tag{33}$$

and, if $n \equiv 3(mod\,4)$,

$$GM_{a,n} \equiv 1(mod\,10) \text{ if } a \equiv 0(mod\,5) \text{ or } 1(mod\,5) \tag{34}$$
$$GM_{a,n} \equiv 7(mod\,10) \text{ if } a \equiv 2(mod\,5) \text{ or } 4(mod\,5) \tag{35}$$
$$GM_{a,n} \equiv 9(mod\,10) \text{ if } a \equiv 3(mod\,5). \tag{36}$$

Proof. Let a, n, r, α be natural integers with $a \geq 2$, $0 \leq \alpha \leq 4$, and n prime, $n \geq 3$. Writing $a \equiv \alpha(\text{mod}\,5)$ and taking the congruence modulo 5 of $GM_{a,n}$ (2) yields $GM_{a,n} \equiv (\alpha^n - (\alpha-1)^n)(\text{mod}\,5)$.

(i) For the first case $n \equiv 1(\text{mod}\,4)$ and writing $n = 4r+1$, (33) is immediate as $GM_{a,n} \equiv \left(\alpha^{4r+1} - (\alpha-1)^{4r+1}\right)(\text{mod}\,5) \equiv 1(\text{mod}\,5)$ for the five cases of $\alpha = 0$ to 4. As all $GM_{a,n}$are odd, all $GM_{a,(4r+1)}$ must be congruent to 1 modulo 10.

(ii) For the second case $n \equiv 3(\text{mod}\,4)$ and writing $n = 4r+3$, one has $GM_{a,n} \equiv \left(\alpha^{4r+3} - (\alpha-1)^{4r+3}\right)(\text{mod}\,5)$, yielding $GM_{a,(4r+3)} \equiv 1(\text{mod}\,5)$ for $\alpha = 0$ and 1, $GM_{a,(4r+3)} \equiv 2(\text{mod}\,5)$ for $\alpha = 2$ and 4, and $GM_{a,(4r+3)} \equiv -1(\text{mod}\,5)$ for $\alpha = 3$. As all $GM_{a,n}$are odd, it follows that (34) to (36) hold. □

2.4. Congruence Properties of Generalized Mersenne Numbers and Their Factors

2.4.1. Generalization of a Second Theorem on Mersenne Numbers

For generalized Mersenne composites, let us note generally their positive natural integer factors c_i such as

$$GM_{a,n} = c_1^{e_1} c_2^{e_2} \ldots c_i^{e_i} \ldots \tag{37}$$

where e_i are positive natural integer exponents. A theorem on factors of Mersenne numbers states, with the notations in this paper, that if n is an odd prime and if c_i divides M_n, then $c_i \equiv 1(\text{mod}\,n)$ and $c_i \equiv \pm 1(\text{mod}\,8)$.

The first part is not only obviously true for all M_n by (3), but can be generalized to $c_i \equiv 1(\text{mod}\,2n)$. The second part is also obviously correct for factors c_i of Mersenne numbers M_n, noting that first, all $M_n \equiv -1(\text{mod}\,8)$ for $n \geq 3$; second, at least one of the factors c_i of the Mersenne number $M_n = GM_{2,n}$ must be congruent to -1 modulo 8; and third, that the sum of exponents e_i of factors c_i which are congruent to the -1 modulo 8 must be odd. This is, however, no longer correct for all $GM_{a,n}$ with $a > 2$.

This theorem can be generalized in two steps. The first part is generalized in the following theorem.

Theorem 5. *For all natural integer bases $a \geq 2$, if n is an odd prime and if a positive natural integer c_i divides $GM_{a,n}$, then*

$$c_i \equiv 1(mod\,2n). \tag{38}$$

Proof. Let a, b, n, m, i, k, c_i, f_i, f_i', λ_i, r_i, p, q be natural integers with $a \geq 2$, n prime, $n \geq 3$, $m > 1$, $k > 0$, $c_i \geq 1$, p prime, $q > 0$ and $1 \leq i \leq q$.

Proving this theorem is equivalent to show that all prime integer factors of $GM_{a,n}$ are of the form

$$c_i = 2nf_i + 1. \tag{39}$$

Let us assume first the contrary, i.e., that the prime integer factors c_i of $GM_{a,n}$ are not of the form (39). For q factors c_i (the case where their exponents $e_i \neq 1$ can be treated similarly), one has from (9) and (25)

$$GM_{a,n} = c_1 c_2 \ldots c_q = 2nQ_n(a) + 1 \equiv 1(\text{mod}\, 2n). \tag{40}$$

Let us then write generally

$$c_i = 2nf_i' + \lambda_i \tag{41}$$

with the condition that the product

$$\lambda_1 \lambda_2 \ldots \lambda_q \equiv 1(\text{mod}\, 2n) \tag{42}$$

i.e., that all λ_i is such that $\lambda_i \equiv 1(\text{mod}\, 2n)$ or that an even number of λ_i are such that $\lambda_i \equiv -1(\text{mod}\, 2n)$, which means that there exist natural integers r_i such as $\lambda_i = 2nr_i + 1$ or $\lambda_i = 2nr_i - 1$. Then, one can write the factors c_i as

$$c_i = 2n\left(f_i' + r_i\right) + 1 \;\text{ or }\; c_i = 2n\left(f_i' + r_i\right) - 1. \tag{43}$$

Let us now assume that an even number of prime factors are of the form $c_i = 2nf_i - 1$. But this is not possible, as it was proven (see [14], p. 267, Nr 2) that all prime factors of $(a^m - b^m)$, with $a > b$ and $m > 1$, are of the form $(mk + 1)$. This is simply shown considering that if a prime p divides $(a^m - b^m)$, and if p does not divide a and b, then by Fermat's theorem, p divides $\left(a^{p-1} - 1\right)$ and $\left(b^{p-1} - 1\right)$ and then also $\left(a^{p-1} - b^{p-1}\right)$ and therefore m divides $(p - 1)$, i.e., $p = mk + 1$.

For $b = (a - 1)$, $m = n$ prime and $k = 2f_i$, it is seen directly that n divides $(c_i - 1)$ if c_i is of the form (39). Therefore, all prime integer factors of $GM_{a,n}$ are of the form (39). Furthermore, composite factors of $GM_{a,n}$ are also obviously of the form (39), being the product of prime factors of the form (39). □

Note that for $n = 2$, all factors c_i of $GM_{a,2}$ are obviously such that $c_i \equiv \pm 1(\text{mod}\, 4)$.

The second part of the generalization of the theorem on factors of Mersenne numbers needs to specify the congruence of $GM_{a,n}$ modulo 8, as in the following theorem.

Theorem 6. *For all natural integer bases $a \geq 2$ and all prime integer exponents $n \geq 3$, all $GM_{a,n}$ are such that*

$$GM_{a,n} \equiv 1(mod\, 8) \quad \text{if } \; a \equiv 0(mod\, 8) \;\text{ or }\; 1(mod\, 8) \tag{44}$$
$$GM_{a,n} \equiv -1(mod\, 8) \;\text{ if }\; a \equiv -1(mod\, 8) \;\text{ or }\; 2(mod\, 8) \tag{45}$$
$$GM_{a,n} \equiv 3(mod\, 8) \quad \text{if } \; a \equiv -2(mod\, 8) \;\text{ or }\; 3(mod\, 8) \tag{46}$$
$$GM_{a,n} \equiv -3(mod\, 8) \;\text{ if }\; a \equiv -3(mod\, 8) \;\text{ or }\; 4(mod\, 8) \tag{47}$$

and the factors c_i of $GM_{a,n}$ are such that $c_i \equiv \pm 1(mod\, 8)$ or $\pm 3(mod\, 8)$ such that their product satisfy above relations.

Proof. Let a, n, α be natural integers with $a \geq 2$, n prime, $n \geq 3$ and $0 \leq \alpha < 8$. The proof of the first part of this theorem is immediate. Consider $a \equiv \alpha(\text{mod}\, 8)$; one has for α even, $a^n \equiv 0(\text{mod}\, 8)$ and for α odd, $a^n \equiv \alpha(\text{mod}\, 8)$. It yields directly relations (44) to (47). The second part of the theorem on the congruence of factors c_i of $GM_{a,n}$ is then obvious. □

The factorization of the first composites $GM_{a,n}$ is indicated in Table 2 for n primes, $3 \leq n \leq 11$. It is seen that all the factors c_i of composites $GM_{a,n}$ are of the form (39) and are either $GM_{a,n} \equiv \pm 1(\text{mod}\, 8)$ or $\pm 3(\text{mod}\, 8)$ such that their products satisfy relations (44) to (47).

Composite $GM_{a,n}$ can be written generally in function of their prime integer factors, from (37) and (39),

$$GM_{a,n} = c_1^{e_1} c_2^{e_2} \ldots c_i^{e_i} \ldots = (2nf_1+1)^{e_1}(2nf_2+1)^{e_2} \ldots (2nf_i+1)^{e_i} \ldots \tag{48}$$

In the case of more than two prime integer factors and for exponents $e_i \neq 1$, a composite $GM_{a,n}$ can also be written in all generality as the product of two factors not necessarily primes and with their exponents $e_i = 1$, as any combination of products of factors c_i of the form (39) will be of the same form (39):

$$GM_{a,n} = c_1 c_2 = (2nf_1+1)(2nf_2+1). \tag{49}$$

Therefore, a corollary of the above Theorem 7 is as follows.

Corollary 2. *For all natural integer bases $a \geq 2$ and all prime integer exponents $n \geq 3$, a natural integer $c_i = (2nf_i+1)$ divides a $GM_{a,n}$ if and only if the integer function $Q_n(a)$ associated to the $GM_{a,n}$ is such that*

$$Q_n(a) \equiv f_i (mod\, c_i) \tag{50}$$

for all factors c_i and where f_i are natural integers.

Proof. Let a, n, r be natural integers with $a \geq 2$, n prime, $n \geq 3$.

Relation (50) obviously holds whether $GM_{a,n}$ is prime or composite. For two factors like in (49), one has

$$GM_{a,n} = 2nQ_n(a) + 1 = (2nf_1+1)(2nf_2+1) = 2n(f_2c_1 + f_1) + 1$$

yielding immediately (50). If $GM_{a,n}$ is prime, then $f_2 = 0$ and $f_1 = Q_n(a)$.

Conversely, if the integer function $Q_n(a)$ is such that (50) holds with $c_1 = (2nf_1+1)$, then it exists an integer r such as

$$Q_n(a) = rc_1 + f_1 \tag{51}$$

yielding

$$2nQ_n(a) + 1 = 2nrc_1 + 2nf_1 + 1 = (2nf_1+1)(2nr+1) = c_1c_2 = GM_{a,n} \tag{52}$$

meaning that c_1 divides $GM_{a,n}$ for an appropriate choice of the integer r, which is here f_2 in the second factor c_2 of $GM_{a,n}$. This relation (50) is true whether the factors c_1 and c_2 are composites or primes of the form (39). □

From Table 2, it is seen that the integers f_1, f_2, ..., f_i, ... in (48) for a particular prime exponent n are increasing from one composite number to the next for increasing values of the base a, and can be found in function of the integer functions $Q_n(a)$.

2.4.2. Generalization of a Third Theorem on Mersenne Numbers (Euler Theorem)

Another theorem on Mersenne numbers was stated by Euler in 1750. With the notations in this paper, it reads as follows: if n is prime, $n \equiv 3(\text{mod}\,4)$, then $(2n+1)$ divides M_n if and only if $(2n+1)$ is a prime; in this case, if $n > 3$, then M_n is composite. This means that for $n \equiv 3(\text{mod}\,4)$ and prime, $M_n = GM_{2,n}$ has the factor $c_1 = (2nf_1+1)$ with $f_1 = 1$, and that c_1 in this case is prime. This is exactly the case for $n = 3$ and $M_3 = GM_{2,3} = 7$; $n = 11$ and $M_{11} = GM_{2,11} = 2047 = 23 \cdot 89$; and so on. This can be generalized for all $GM_{a,n}$ for odd primes n, irrespective of n being congruent to $3(\text{mod}\,4)$ or not, in a following theorem, showing that a natural integer c_i divides $GM_{a,n}$ if and only if $c_i = (2nf_i+1)$ is prime or a composite formed by the product of primes of the form $(2nj+1)$ for some natural integer values of f_i and with j natural integers.

It is important to realize that not all integer values of f_i will do, only those that render the factor c_i prime or composite of the form $(2nf_i+1)$ will be acceptable. All other integer values of f_i are excluded and are called excluded values. The following Lemma is demonstrated, giving the form that factors c_i cannot take and the form of excluded values of f_i.

Lemma 1. *For all natural integer bases $a \geq 2$ and all prime integer exponents $n \geq 3$, a natural integer $c_i = (2nf_i+1)$ divides a $GM_{a,n}$ if c_i and f_i are different from excluded values, i.e., different, respectively, from either (i)*

$$c_i \not\equiv 0(mod\,(2nk+1)) \quad \text{and} \quad f_i \not\equiv k(mod\,(2nk+1)) \tag{53}$$

for positive natural integers $k = 2nuv + u\varepsilon + v\delta + r$, with u, v and r positive natural integers such as $uv \neq 0$, ε and δ integers $\neq 0$ and $\neq 1$ and such as $\varepsilon\delta \equiv 1(mod\,2n) = 2nr+1$; or (ii)

$$c_i \not\equiv 0(mod\,(2nk-1)) \quad \text{and} \quad f_i \not\equiv -k(mod\,(2nk-1)) \tag{54}$$

for positive natural integers k; or (iii)

$$c_i \not\equiv 0(mod\,(2nk \pm t)) \quad \text{and} \quad f_i \not\equiv (\alpha + k\beta)(mod\,(2nk+\gamma)) \tag{55}$$

for natural integers k, for odd natural integers t such that $1 < t < n$, for integers α, β, γ, with β and γ odd integers and $2n\alpha + 1 = \beta\gamma$.

Proof. Let a, n, i, j, k, c_i, f_i, s, u, v, x, y be natural integers with $a \geq 2$, n prime, $n \geq 3$, and α, β, γ, δ, ε, r integers and $\delta \neq 0$ and $\varepsilon \neq 0$.

From Theorem 6, factors c_i of a $GM_{a,n}$ are

$$c_i = 2nf_i + 1 \equiv 1(\text{mod}\,2n). \tag{56}$$

Let us assume in all generality that f_i can be written as

$$f_i \equiv x(\text{mod}\,y) \tag{57}$$

for yet unknown natural integers x and y. For a given prime n, for f_i to be excluded values, (56) must not be verified for all bases a. Among all possible values of f_i, it will be the case if in (56)

$$c_i = 2nf_i + 1 \equiv 0(\text{mod}\,y) \tag{58}$$

meaning that

$$2nx + 1 \equiv 0(\text{mod}\,y) \tag{59}$$

is a multiple of y. Writing in all generality $x = (\alpha + k\beta)$ and $y = (2nk+\gamma)$, one has from (57)

$$f_i \equiv (\alpha + k\beta)(\text{mod}\,(2nk+\gamma)) = (2nk+\gamma)s + (\alpha + k\beta) \tag{60}$$

with α, β, γ integers and k and s natural integers. Replacing in (59) yields

$$2n(\alpha + k\beta) + 1 \equiv 0(\text{mod}\,(2nk+\gamma)) \tag{61}$$

or

$$\beta\left(\left(\frac{2n\alpha+1}{\beta}\right) + 2nk\right) \equiv 0(\text{mod}\,(2nk+\gamma)) \tag{62}$$

which gives the condition

$$2n\alpha + 1 = \beta\gamma \tag{63}$$

where β and γ are obviously odd integers, either positive and/or negative depending on the sign of α. The factors c_i read then from (58) and (60) with (63)

$$c_i = 2n((2nk+\gamma)s + (\alpha + k\beta)) + 1 = (2nk+\gamma)(2ns+\beta) \tag{64}$$

All f_i of the form (60) are excluded values and all c_i of the form (64) cannot be factors of $GM_{a,n}$ for every integer α, β, γ complying with (63) and for all natural integers k, except for the following specific cases.

(i) First, for the triplet $(\alpha,\beta,\gamma) = (0,1,1)$ verifying (63), f_i (60) and factors c_i (64) read, respectively,

$$f_i \equiv k(\mathrm{mod}\,(2nk+1)) = (2nk+1)s + k \tag{65}$$

$$c_i = 2n((2nk+1)s + k) + 1 = (2nk+1)(2ns+1). \tag{66}$$

If for certain positive integers k, $(2nk+1)$ is prime, then by Theorem 6, c_i (66) are factors of a $GM_{a,n}$ and f_i (65) are not excluded values.

If for other positive integers k, $(2nk+1)$ is composite, it can be written as

$$(2nk+1) = (2nu+\delta)(2nv+\varepsilon) \tag{67}$$

with the obvious condition

$$\delta\varepsilon \equiv 1(\mathrm{mod}\,2n) = 2nr+1 \tag{68}$$

where u and v are natural integers with u and v not simultaneously null; δ, ε and r are integers with $\delta \neq 0$ and $\varepsilon \neq 0$; and

$$k = 2nuv + u\varepsilon + v\delta + r. \tag{69}$$

As k must be a natural integer, only the values of δ and ε complying with (68) must be considered. For $\delta = \varepsilon = 1$ (i.e., $r = 0$), $k = 2nuv + u + v$ and the factors of $(2nk+1)$ are

$$(2nk+1) = (2nu+1)(2nv+1) \tag{70}$$

showing that f_i (65) with (70) are not excluded values, similarly to the above case of $(2nk+1)$ being prime.

For all the other cases of values of k in (69) with δ and ε integers $\neq 0$ and $\neq 1$, and complying with (68), the factors c_i from (66) read

$$c_i = (2ns+1)(2nu+\delta)(2nv+\epsilon) \tag{71}$$

which, by Theorem 6, cannot be factors of a $GM_{a,n}$ and the corresponding f_i (65) are excluded values. For example, with $\delta = \varepsilon = -1$ (i.e., $r = 0$), the factors of $(2nk+1)$ are $(2nu-1)(2nv-1)$, showing from (66) that $c_i = (2ns+1)(2nu-1)(2nv-1)$ cannot be factors of a $GM_{a,n}$ and that the corresponding f_i are excluded values.

(ii) Second, for the triplet $(\alpha,\beta,\gamma) = (0,-1,-1)$ verifying (63), f_i (60) and factors c_i (64) read, respectively,

$$f_i \equiv -k(\mathrm{mod}\,(2nk-1)) = (2nk-1)s - k \tag{72}$$

$$c_i = 2n((2nk-1)s - k) + 1 = (2nk-1)(2ns-1) \tag{73}$$

showing again by Theorem 6 that c_i (73) cannot be factors of a $GM_{a,n}$ and that f_i (72) are excluded values for all positive integers k.

(iii) Third, for the general case where $\alpha \neq 0$, from (63), both β and γ are obviously $\neq 1$, and therefore, again by Theorem 6, c_i (64) cannot be factors of a $GM_{a,n}$ and all f_i (60) are excluded values for all natural integers k.

Summarizing, the excluded values of f_i and the excluded forms of factors c_i are, respectively, (53) for positive integers k (69) with δ and ε integers $\neq 0$ and $\neq 1$; (54) for all positive integers k; and (55) for all integers α, all odd integers β and γ complying with (63), all natural integers k and all t odd integers such that $1 < t < n$, as, from the form of factors c_i (64),

$$t \equiv \beta (\mathrm{mod}\, 2nk) \quad \text{or } t \equiv \gamma (\mathrm{mod}\, 2nk). \tag{74}$$

The excluded forms of factors c_i (55) are always composites and the product of at least two factors, which are multiple of integers of the form $(2nj - 1)$ and/or $(2nj \pm t)$ with j natural integers and at least once $j = k$. □

We can now prove Theorem 7 as follows.

Theorem 7. *For all natural integer bases $a \geq 2$ and all prime integer exponents $n \geq 3$, a natural integer c_i divides $GM_{a,n}$ if and only if, for some natural integer values of f_i, $c_i = (2nf_i + 1)$ is prime or a composite formed by the product of primes of the form $(2nj + 1)$, with i and j natural integers and c_i and f_i different from excluded values given in (53) to (55).*

Proof. Let a, n, i, j, k, c_i, f_i be natural integers with $a \geq 2$, n prime, $n \geq 3$.

The first part of the demonstration is quite straightforward as from Theorem 6 above, all natural integer prime and composite factors of $GM_{a,n}$ are of the form (39).

Conversely, if a natural integer $c_1 = (2nf_1 + 1)$ is prime or a composite formed by the product of primes of the form $(2nj + 1)$, then, for a suitable choice of an integer f_2, a natural integer function Φ_n can be found and written as

$$\Phi_n = f_2(2nf_1 + 1) + f_1. \tag{75}$$

The suitable choice of the integer f_2 means here that it must not be an excluded value specifically for the prime exponent n as shown in above Lemma, i.e., that $c_2 = (2nf_2 + 1)$ must itself be either a prime or a composite formed by the product of primes of the form $(2nj + 1)$. Relation (75) then yields

$$\Phi_n \equiv f_1 (\mathrm{mod}\, (2nf_1 + 1)) \tag{76}$$

and by Corollary 2 above, $c_1 = (2nf_1 + 1)$ divides $GM_{a,n} = (2n\Phi_n + 1)$, i.e., there is a base a for which the polynomial $Q_n(a)$ in (4) specific for each prime exponent n is equal to Φ_n (75). □

We emphasize again that not all integer values of f_1 and f_2 will do, and that the integer f_2 must be chosen suitably, such that the factors $c_1 = (2nf_1 + 1)$ and $c_2 = (2nf_2 + 1)$ are prime or composite formed by the product of primes of the form $(2nj + 1)$. All other values of f_1 and f_2 are excluded values, as shown in Lemma 1.

2.4.3. Theorem on Congruence of Coefficients f_1 and f_2

The form of the integers f_1 and f_2 in the factors c_1 and c_2 of composite $GM_{a,n}$ can be determined in function of the exponent n, the base a and the factors c_1 and c_2 by the following theorem.

Theorem 8. *If a composite $GM_{a,n}$ has $c_1 = (2nf_1 + 1)$ and $c_2 = (2nf_2 + 1)$ as two factors, then $f_1 \equiv u(\mathrm{mod}\, 4)$ and $f_2 \equiv v(\mathrm{mod}\, 4)$ with u and $v = 0, 1, 2$ or 3, depending on the congruence of $n(\mathrm{mod}\, 4)$ and on the congruence of $a(\mathrm{mod}\, 8)$, as shown in Table 3.*

Table 3. Congruence of natural integers f_1 and f_2 (mod 4).

$c_1 \equiv ...$ (mod 8)	$f_1 \equiv ...$ (mod 4)	if $a \equiv 0$ or $1(\mathrm{mod}\,8)$, $f_2 \equiv ...$ (mod 4)	if $a \equiv 2$ or $7(\mathrm{mod}\,8)$, $f_2 \equiv ...$ (mod 4)	if $a \equiv 3$ or $6(\mathrm{mod}\,8)$, $f_2 \equiv ...$ (mod 4)	if $a \equiv 4$ or $5(\mathrm{mod}\,8)$, $f_2 \equiv ...$ (mod 4)
For $n \equiv 1(\mathrm{mod}\,4)$					
1	0	0	3	1	2
3	1	1	2	0	3
5	2	2	1	3	0
7	3	3	0	2	1
For $n \equiv 3(\mathrm{mod}\,4)$					
1	0	0	1	3	2
3	3	3	2	0	1
5	2	2	3	1	0
7	1	1	0	2	3

The demonstration of this theorem is based on the above Theorems 6 and 7.

Proof. Let $a, n, i, j, c_i, f_i, u, v$ be natural integers with $a \geq 2$, n prime, $n \geq 3$ and α, β, γ integers. Let c_1 and c_2 be the two factors of $GM_{a,n} = c_1 c_2$. From Theorem 7, c_1 and c_2 are primes of the form $(2nf_1 + 1)$ and/or composites of the form of a product of integers $(2nj + 1)$. From Theorem 6, one has

$$GM_{a,n} \equiv \alpha(\mathrm{mod}\,8) \tag{77}$$

with $c_1 \equiv \beta(\mathrm{mod}\,8)$ and $c_2 \equiv \gamma(\mathrm{mod}\,8)$, where α, β and γ take values either ± 1 or ± 3, with the obvious condition that

$$\alpha \equiv \beta\gamma(\mathrm{mod}\,8) \tag{78}$$

which then yields by Theorem 6

$$\beta = \gamma \text{ for } \alpha = +1 \text{ i.e., for } a \equiv 0(\mathrm{mod}\,8) \text{ or } 1(\mathrm{mod}\,8) \tag{79}$$

$$\beta = -\gamma \text{ for } \alpha = -1 \text{ i.e., for } a \equiv 2(\mathrm{mod}\,8) \text{ or } 7(\mathrm{mod}\,8) \tag{80}$$

$$\beta = -\gamma + 4 \text{ for } \alpha = +3 \text{ i.e., for } a \equiv 3(\mathrm{mod}\,8) \text{ or } 6(\mathrm{mod}\,8) \tag{81}$$

$$\beta = \gamma - 4 \text{ for } \alpha = -3 \text{ i.e., for } a \equiv 4(\mathrm{mod}\,8) \text{ or } 5(\mathrm{mod}\,8). \tag{82}$$

For

$$c_1 = 2nf_1 + 1 \equiv \beta(\mathrm{mod}\,8) \tag{83}$$

one has for

$$n \equiv 1(\mathrm{mod}\,4): \quad f_1 \equiv \left(\frac{\beta - 1}{2}\right)(\mathrm{mod}\,4) \equiv u(\mathrm{mod}\,4) \tag{84}$$

$$n \equiv 3(\mathrm{mod}\,4): \quad f_1 \equiv \left(\frac{1 - \beta}{2}\right)(\mathrm{mod}\,4) \equiv u(\mathrm{mod}\,4) \tag{85}$$

and $f_2 \equiv v(\mathrm{mod}\,4)$ is found by replacing in (84) and (85) β in function of γ from (79) to (82) depending on the prime exponent n and the base a. Hence, the congruences given in Table 3 hold. □

Note that for Mersenne numbers (i.e., for $a = 2$ in Table 3), $c_1 \equiv 1(\mathrm{mod}\,8)$ or $7(\mathrm{mod}\,8)$, yielding that f_1 and f_2 are congruent to $0(\mathrm{mod}\,4)$ and/or $3(\mathrm{mod}\,4)$ for $n \equiv 1(\mathrm{mod}\,4)$, and f_1 and f_2 are congruent to $0(\mathrm{mod}\,4)$ and/or $1(\mathrm{mod}\,4)$ for $n \equiv 3(\mathrm{mod}\,4)$.

3. Results and Discussion

Distributions of primes and composites in generalized Mersenne numbers are further investigated in companion papers. However, generalized Mersenne numbers as presented in this paper are useful to approach the problem of why most of the Mersenne numbers with prime exponents are not themselves primes. It was mentioned in the introduction that composite and prime generalized Mersenne numbers appear apparently at random for different values of the exponent n and the base a. It is seen also that prime generalized Mersenne numbers can be found for larger values of the base a for exponents n that yield Mersenne composites, like, e.g., for $n = 11, 23, 29, \ldots$. It appears that some exponents n are less "productive" than others to yield generalized Mersenne primes. The reason for this is still unknown, but it shows that Mersenne numbers that are composite for prime exponents are nothing exceptional and are simply generalized Mersenne composites for $a = 2$. Sequences of generalized Mersenne numbers, primes, bases, and exponents can be found online at the Online Encyclopedia of Integer Sequences (OEIS) [19]; see Table 4.

Table 4. OEIS references of sequences of generalized Mersenne numbers, primes, bases and exponents for k integers.

n	$GM_{a,n}$ Numbers	$GM_{a,n}$ Primes				
		Primes	a	**# for** $a \leq 10^k$	**#** $< 10^k$	$10^{k-1} <$ **#** $< 10^k$
2	A005408	A000040	–	–	A006880	A006879
3	A003215	A002407	A002504	A221794	A113478	A221792
5	A022521	A121616	A121617	A221849	A221846	A221847
7	A022523	A121618	A121619	A221980	A221977	A221978
11	A022527	A189055	A211184	A221986	A221983	A221984
13	A022529	–	–	–	–	–
17	A022533	–	–	–	–	–
19	A022535	–	–	–	–	–
23	A022539	–	–	–	–	–

Notes: # means "Number of $GM_{a,n}$ primes". For $n = 2$, the first prime, 2, must be removed from the sequences indicated in the first row as $GM_{a,2}$ generates only all the odd integers. In some sequences, a shift of one unity must be applied.

The density of Mersenne primes is also very low. Let us consider the largest known Mersenne prime $M_{82589933} = \left(2^{82589933} - 1\right)$, having 24862048 digits.

If we compare the number of known Mersenne primes, 51, first to the number of all the primes less than $10^{24862048}$ that can be approximated from the prime number theorem as $\Pi\left(10^{24862048}\right) \approx 10^{24862048} / \ln\left(10^{24862048}\right)$, i.e., approximately $1.75 \cdot 10^{24862042}$, and second to the number of Mersenne numbers with prime exponents, i.e., the number of primes less than 82589933, i.e., $\Pi(82589933) \approx 82589933 / \ln(82589933)$, or approximately 4530590, we see that the density of Mersenne primes is extremely low, in the order of $2.1 \cdot 10^{-24862041}$ and $1.1 \cdot 10^{-5}$, respectively, for the first and second cases.

Mersenne primes are used in cryptography (see, e.g., [8,20–24]). But to fix the ideas, only medium-sized Mersenne primes are used in cryptography. So the search for larger Mersenne primes does not have applications in cryptography. Generally speaking, there are two applications of Mersenne primes within cryptography [25]:

- As a modulus within a prime elliptic curve: for example, the Mersenne prime $\left(2^{521} - 1\right)$ is used to define an elliptic curve.
- In the Carter–Wegman Counter (CWC) mode [26], the Mersenne prime $\left(2^{127} - 1\right)$ is used to define a universal hash function consisting of evaluating a polynomial modulo the Mersenne prime $\left(2^{127} - 1\right)$.

In both cases, the special property that is taken advantage of is that Mersenne primes (rather than another prime of approximately the same size) make computing the modulo operation $x \bmod \left(2^{521} - 1\right)$ or $x \bmod \left(2^{127} - 1\right)$ easy by the linear-feedback shift register (LFSR). More generally, performing modular reduction modulo a Mersenne prime does not modify the hamming weight of the result.

On the other hand, in asymmetric key cryptography, a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public keys and private keys are different. Even if the public key is known by everyone, the intended receiver can only decode it because he alone knows his private key. The most popular asymmetric key cryptography algorithm is the Rivest–Shamir–Adleman (RSA) algorithm [27]. The practical difficulty of factoring the product of two large prime numbers is what makes the RSA algorithm secure.

As seen, the number of Mersenne primes is relatively limited, and *a fortiori*, those of medium size are even less. As an alternative for asymmetric key cryptography, we propose to use generalized Mersenne primes, which are more frequent even for small prime exponents and for which both the base a and the exponent n can be used either as public keys or secret keys.

4. Conclusions

It was shown that with the proposed generalization of Mersenne numbers, for any natural integer base a, generalized Mersenne numbers are in general such that $(GM_{a,n} - 1)$ are even and divisible by n, a and $(a-1)$ for any odd prime exponent n and by $(a(a-1)+1)$ for any prime exponent $n > 5$. The remaining factor is a function of triangular numbers of $(a-1)$, specific to each prime exponent n. Four theorems on Mersenne numbers were generalized for generalized Mersenne numbers and four new theorems were demonstrated, allowing one to show first that $(GM_{a,n} - 1)$ are divisible by 6, and more precisely, $GM_{a,n}$ are congruent to $1 (\bmod 12)$ or $7 (\bmod 12)$ depending on the congruence of the base $a (\bmod 4)$; second, that $(GM_{a,n} - 1)$ are divisible by 10 if $n \equiv 1 (\bmod 4)$ and, if $n \equiv 3 (\bmod 4)$, $GM_{a,n} \equiv 1 (\bmod 10)$, or $7 (\bmod 10)$ or $9 (\bmod 10)$ depending on the congruence of the base $a (\bmod 5)$; third, that all factors c_i of $GM_{a,n}$ are of the form $(2nf_i + 1)$ with f_i natural integers such that c_i is prime itself or the product of primes of the form $(2nj + 1)$ with j natural integer; fourth, that for odd prime exponents n, all $GM_{a,n}$ are periodically congruent to either $\pm 1 (\bmod 8)$ or $\pm 3 (\bmod 8)$ depending on the congruence of the base $a (\bmod 8)$; and fifth, that the factors of a composite $GM_{a,n}$ is of the form $(2nf_i + 1)$ with $f_i \equiv u (\bmod 4)$ and u being either 0, 1, 2 or 3 depending on the congruence of the exponent $n (\bmod 4)$ and on the congruence of the base $a (\bmod 8)$. Note that alternate proofs for Theorems 1, 2, 4, 5 and 7, and another development of $GM_{a,n}$ in embedded products are given in the online version of the paper [28]. Finally, the potential use of generalized Mersenne primes in cryptography has been shortly addressed.

Distributions of primes and composites in generalized Mersenne numbers are further investigated in companion papers.

Funding: This research received no external funding.

Data Availability Statement: There are no data associated with this work.

Acknowledgments: The author wishes to thank an anonymous reviewer for suggesting shorter proofs of some theorems. The help of Prof. D. Huylebrouck is acknowledged. This research was conducted under the good auspice of the European Space Agency Technical and Research Centre (The Netherlands).

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Ribenboim, P. *The Book of Prime Number Records*, 2nd ed.; Springer: New York, NY, USA, 1989; pp. 75–81.
2. Caldwell, C.K. Mersenne Primes: History, Theorems and Lists. Available online: http://primes.utm.edu/mersenne/index.html#known (accessed on 10 January 2023).
3. Weisstein, E.W. Mersenne Prime, from Mathworld—A Wolfram Web Resource. Available online: http://mathworld.wolfram.com/MersennePrime.html (accessed on 10 January 2023).
4. Great Internet Mersenne Prime Search GIMPS. Available online: https://www.mersenne.org/primes/ (accessed on 10 January 2023).
5. Crandall, R.E. Method and Apparatus for Public Key Exchange in a Cryptographic System. U.S. Patent # 5,159,632, 27 October 1992.
6. Solinas, J. *Generalized Mersenne Numbers*; Technical Report CORR 99-39; University of Waterloo: Waterloo, ON, Cananda, 1999.
7. Solinas, J. Cryptographic Identification and Digital Signature Method Using Efficient Elliptic Curve. U.S. Patent # 6,898,284, 24 May 2005.

8. Solinas, J.A. Mersenne Prime. In *Encyclopedia of Cryptography and Security*; Van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011. [CrossRef]
9. De Jesus Angel, J.; Morales-Luna, G. Counting Prime Numbers with Short Binary Signed Representation. 2006. Available online: https://eprint.iacr.org/2006/121.pdf (accessed on 5 February 2024).
10. Hoque, A.; Saikia, H.K. On Generalized Mersenne Prime. *SeMA* **2014**, *66*, 1–7. [CrossRef]
11. Hoque, A.; Saikia, H.K. On generalized Mersenne Primes and class-numbers of equivalent quadratic fields and cyclotomic fields. *SeMA* **2015**, *67*, 71–75. [CrossRef]
12. Deng, L.Y. Generalized Mersenne Prime Number and Its Application to Random Number Generation. In *Monte Carlo and Quasi-Monte Carlo Methods 2002*; Niederreiter, H., Ed.; Springer: Berlin/Heidelberg, Germany, 2004. [CrossRef]
13. Pletser, V. Generalized Mersenne prime numbers: Characterization and distributions. In Proceedings of the 4th WSEAS International Conference on Applied Mathematics, La Valette, Malta, 1–3 September 2003; WSEAS Transactions on Mathematics: Athens, Greece, 2003; Volume 2, pp. 78–82, ISSN 1109-2769. Available online: https://www.researchgate.net/publication/257880586_Generalized_Mersenne_prime_numbers_characterization_and_distributions (accessed on 5 February 2024).
14. Sierpinski, W. *Elementary Theory of Numbers*, 2nd ed.; Schinzel, S., Ed.; Elsevier: Amsterdam, The Netherlands; PWN: Warsaw, Poland, 1988; pp. 360–362.
15. Conway, J.H.; Guy, R.K. *The Book of Numbers*; Springer: New York, NY, USA, 1996; pp. 38–56.
16. Ram, B. Common Factors of $\frac{n!}{m!(n-m)!}$, $(m = 1, 2, ..., n-1)$. *J. Indian Math. Club Madras* **1909**, *1*, 39–43.
17. Dickson, L.E. *History of the Theory of Numbers, Vol.1: Divisibility and Primality*; Chap IX; Dover Publ.: New York, NY, USA, 2005; pp. 263–278.
18. Catalan, E. Arithmetical proofs. *Am. Math. Mon.* **1911**, *18*, 41–43.
19. Sloane, N.J.A. The Online Encyclopedia of Integer Sequences. Available online: https://oeis.org/ (accessed on 5 February 2024).
20. Kalita, J.; Hoque, A.; Kalita, H. A new cryptosystem using generalized Mersenne primes. *SeMA* **2016**, *73*, 77–83. [CrossRef]
21. Coron, J.S.; Gini, A. Improved cryptanalysis of the AJPS Mersenne based cryptosystem. *J. Math. Cryptol.* **2020**, *14*, 218–223. [CrossRef]
22. Aggarwal, D.; Joux, A.; Prakash, A.; Santha, M. A new public-key cryptosystem via Mersenne numbers. In *Advances in Cryptology—CRYPTO 2018, Lecture Notes in Computer Science 10993*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 459–482. Available online: https://link.springer.com/chapter/10.1007/978-3-319-96878-0_16 (accessed on 10 January 2024).
23. Beunardeau, M.; Connolly, A.; Géraud, R.; Naccache, D. *On the Hardness of the Mersenne Low Hamming Ratio Assumption*; Technical Report. Available online: https://eprint.iacr.org/2017/522 (accessed on 31 January 2024).
24. Tiepelt, M.; D'Anvers, J.P. Exploiting Decryption Failures in Mersenne Number Cryptosystems. In Proceedings of the APKC'20: Proceedings of the 7th ACM Workshop on ASIA Public-Key Cryptography, Taipei, Taiwan, 6 October 2020; pp. 45–54. [CrossRef]
25. Cryptography Stack Exchange, What Is the Use of Mersenne Primes in Cryptography. 2014. Available online: https://crypto.stackexchange.com/questions/19759/what-is-the-use-of-mersenne-primes-in-cryptography/19763#19763 (accessed on 5 February 2024).
26. Kohno, T.; Viega, J.; Whiting, D. CWC: A high-performance conventional authenticated encryption mode. In *Fast Software Encryption, Lecture Notes in Computer Science*; Meier, W., Roy, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3017, pp. 408–426. Available online: https://eprint.iacr.org/2003/106.pdf (accessed on 5 February 2024). [CrossRef]
27. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
28. Pletser, V. Global Generalized Mersenne Numbers: Definition, Decomposition, and Generalized Theorems, Preprint. Available online: https://www.preprints.org/manuscript/202402.0545/v1 (accessed on 11 March 2024).