Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 20, 2014, No. 1, 19–26

Arithmetical sequences for the exponents of composite Mersenne numbers

Simon Davis

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

Abstract: 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. A lower probability for the occurrence of composite Mersenne numbers in arithmetical sequences is given.
Keywords: Composite Mersenne numbers, Exponents in arithemetical sequences.
AMS Classification: 11B83, 11N13, 11P83.

1 Introduction

It has been established that, for any prime of the form $p = 4k + 3$ such that $2p + 1$ is a prime, either $p = 3$ or $2^p - 1$ is composite [4][7]. The largest known composite Mersenne numbers have been generated from Sophie Germain primes [6]. The sequence of Mersenne numbers with prime exponents contains an infinite number of composite integers if there are an infinite number of Sophie Germain primes of the form $4k + 3$.

The problem of proving the infinite extent of the sequence of composite Mersenne numbers with prime indices may be examined by determining arithmetical sequences for the exponents. It is found that there are many such sequences which are often characterized by a nontrivial common divisor of the initial term and the difference. The derivation of a sequence with relatively prime parameters is shown to be feasible after an adaptation of established techniques for $m^p - n$, with $m > 2$ and $n > 1$, $gcd(m, n) = 1$, to $2^p - 1$.

2 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 a minimum of 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 a minimum of three consecutive numbers [9], 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, $\frac{\bar{m}}{2^m-1} \cdot \ell_m$ will be included in the j^{th} triangle if

$$\frac{(j-1)(2^m-1)}{K} \leq \bar{m} \leq \frac{j(2^m-1)}{K}. \tag{2.1}$$

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

$$N_m^K = \left[\frac{j(2^m-1)}{K}\right] - \left\{\frac{(j-1)(2^m-1)}{K}\right\} + 1. \tag{2.2}$$

If the partition includes a site on the i^{th} level, where $i \leq n-1$, 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 $j_{m,s}$, $s = 0, 1, ..., K_m$, $j_{m,0} = 1$, $j_{m,1} = \left\{\frac{K}{K_m}\right\}$, $j_{m,2} = \left\{\frac{2K}{K_m}\right\}$, ...,$j_{m,K_{m_K}-1} = \left\{\frac{(K_m-1)K}{K_m}\right\}$, $j_{m,K_m} = K$ such that $T_{j_{m,s}}$, $s \geq 1$, contains an extra site. Since $2^{m+1} - 1 \equiv 2K_m + 1 \ (mod\ K)$, and additional site is located in each of the triangles $T_{j_{m+1,s}}$ with $j_{m+1,0} = 1$, $j_{m+1,1} = \left\{\frac{K}{2K_m+1}\right\}$, $j_{m+1,2} = \left\{\frac{2K}{2K_m+1}\right\}$,..., $j_{m+1,2K_m} = \left\{\frac{2K_mK}{2K_m+1}\right\}$, $j_{m+1,2K_m+1} = K$.

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

$$2^{m_K} - 1 \equiv K_{m_K} \quad (mod\ K) \qquad 1 \leq K_{m_K} \leq K. \tag{2.3}$$

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 $2^{m_K} \equiv K_{m_K}+1\ (mod\ K)$. $2^{m_K+1} \equiv (K_{m_K}+1)\ (mod\ K)$, ..., $2^{n-1} \equiv 2^{n-1-m_K}(K_{m_K}+1)\ (mod\ K)$, the number of extra sites from level $m_K, ...,\ n-1$ is

$$\sum_{i=m_K}^{n-1} 2^{(i-m_K)}2^{m_K} = 2^{m_K}\Bigg[(2^{m_K}-1)+2^{m_K}((2^{m_K}-1)+ \\ ...+2^{m_K}\left((2^{m_K}-1)+2^{m_K}\sum_{i=rm_K}^{n-1}2^{i-rm_K}\right)\Bigg] \tag{2.4}$$

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

$$(K_{m_K}+1)\Big[K_{m_K}+(K_{m_K}+1)(K_{m_K}+(K_{m_K}+1)(K_{m_K}+(K_{m_K}+1)(K_{m_K}+ \\ ...+(K_{m_K}+(K_{m_K}+1)(2^{n-rm_K}-1))\Big] \qquad (mod\ K) \\ = 2^{n-rm_K}(K_{m_K}+1)-(K_{m_K}+1) \qquad (mod\ K). \tag{2.5}$$

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

$$\sum_{i=0}^{m_K-1} 2^i = 2^{m_K}-1 \equiv K_{m_K} \tag{2.6}$$

such that, from levels 0 to $n-1$, these total

$$2^{n-rm_K}(K_{m_K}+1)-1 \qquad (mod\ K). \tag{2.7}$$

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:
$n=11,\ K=23,\ m_K=5,\ K_{m_K}=8,\ r=2,\ 2^{n-rm_K}(K_{m_K}+1)^r-1=161\equiv 0\ (mod\ 23)$;
$n=23,\ K=47,\ m_K=6,\ K_{m_K}=16,\ r=3,\ 2^{n-rm_K}(K_{m_K}+1)^r-1\equiv 0\ (mod\ 47)$;
$n=29,\ K=233,\ m_K=8,\ K_{m_K}=22,\ r=3,\ 2^{n-rm_K}(K_{m_K}+1)^r-1\equiv 0\ (mod\ 233)$;
$n=7,\ K=223,\ m_K=8,\ K_{m_K}=3,\ r=4,\ 2^{n-rm_K}(K_{m_K}+1)^r-1\equiv 0\ (mod\ 13367)$;
$n=43,\ K=431,\ m_K=9,\ K_{m_K}=80,\ r=4,\ 2^{n-rm_K}(K_{m_K}+1)^r-1\equiv 0\ (mod\ 431)$.

Since 2^n-1, $n>6$ has a proper primitive divisor [1][2][10], there exists a factor which has the form 2^m-k, $m\ /|n$, $1<k\leq 2^{m-1}$. 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 in 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 $ord_K(k) \neq 2^m - k$ for any $K \geq 3$ and $1 \leq k \leq 2^{p-1}$, with $2^p - k \not| 2^p - 1$, where p is a prime exponent, or it consists of integers belonging to sequences of the type $a + bn$, $gcd(a, b) = 1$ with $ord_K(k) \neq a$ for any $K \geq 3$ and k, with $1 \leq k \leq 2^{p-1}$, satisfies the same divisibility conditions. Similarly, suppose that p_1 and p_2 are two prime indices such that

$$\begin{aligned} 2^{p_1} - 1 &\equiv x_1 \qquad (mod\, 2^m - k) \\ 2^{p_2} - 1 &\equiv x_2 \qquad (mod\, 2^{m'} - k_2) \end{aligned} \tag{2.8}$$

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

$$\begin{aligned} 2^{p_1+p_2-1} - 1 \equiv \frac{x_1x_2 + x_1 + x_2 + c_1c_2 - 1}{2} + \frac{c_1}{2}(1 + x_2)(2^m - k_1) \\ + \frac{c_2}{2}(1 + x_1)(2^{m'} - k_2) \qquad (mod\, 2^{m+m'-1} - k_3) \\ k_3 = 2^{m-1}k_2 + 2^{m'-1}k_1 - \frac{k_1k_2 - 1}{2}. \end{aligned} \tag{2.9}$$

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

$$\begin{aligned} 2^{p_1+p_2-1} - 1 \equiv \frac{x_1x_2 + x_1 + x_2 + (c_1 - \alpha)(c_2 - \beta) - 1}{2} \\ + \frac{1}{2}c_1(1 + x_2)(2^m - k_1) + \frac{1}{2}c_2(1 + x_1)(2^{m'} - k_2) \\ + \frac{1}{2}(c_1\beta + c_2\alpha - \alpha\beta)(2^m - k_1)(2^{m'} - k_2) \quad (mod\, 2^{m+m'-1} - k_3). \end{aligned} \tag{2.10}$$

Expressing this quadratic form as a product of linear terms,

$$\begin{aligned} \left[(c_1\beta + c_2\alpha - \alpha\beta)\left\{(2^m - 1) + c_2(1 + x_1)(c_1\beta + c_2\alpha - \alpha\beta)^{-1}\right\}\right] \\ \left\{(2^{m'} - k_2) + c_1(1 + x_2)(c_1\beta + c_2\alpha - \alpha\beta)^{-1}\right\} \\ \equiv c_1c_2(c_1\beta + c_2\alpha - \alpha\beta)^{-1}(1 + x_1)(1 + x_2) \\ - (1 + x_1)(1 + x_2) + c_1c_2 - (c_1\beta + c_2\beta - \alpha\beta) + 1 \\ (mod\, 2^{m+m'-1} - k_3) \end{aligned} \tag{2.11}$$

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.

3 Arithmetical sequences for exponents of Mersenne numbers

The conclusions of the method in the second section can be confirmed by an adaptation of the proof of the existence of infinite number of composite integers of the form $m^p - n$, where $m > 2$,

$mn > 1$ [5][7][8], to the Mersenne numbers $2^p - 1$. First, the direct extension of the proof to $2^p - 1$ does not yield prime divisors for an infinite set of prime exponents. Let $m = 2$ and $n = 1$ such that $m^p - n = 2^p - 1$. Suppose that q divides $m^3 n - 1 = 2^3 - 1 = 7$ and p is a prime satisfying the congruence $p \equiv q - 4 \ (mod\ q - 1)$. Then

$$m^3(m^p - n) = m^3(m^{q-4} - n) = m^{q-1} - m^3 n \equiv 1 - m^3 n \equiv 0 \ (mod\ q). \tag{3.1}$$

Since $q \not| \ m$, $q|m^p - n$. Dirichlet's theorem on primes in an arithmetic progression requires $gcd(q - 4, q - 1) = 1$. However, q must equal 7 and the greatest common divisor is 3. Similarly, if $q|m^5 n - 1$, it equals 31 and when $p \equiv q - 6 \ (mod\ q - 1)$, $gcd(q - 6, q - 1) = 5$. Again, the theorem on primes in an arithmetic progression cannot be used to deduce an infinite number of prime exponents of composite Mersenne numbers.

Proposition 1. The sequence of exponents given by $n = q - \ell \ (mod q - 1)$, where q is a prime divisor of $2^\ell - 1$ consists of composite numbers.

Proof. The Mersenne number $2^\ell - 1$, with ℓ prime, only has divisors of the form $k\ell + 1$. Given that the expression $2^\ell(2^{q-\ell-1} - 1)$ is being considered, $q - 1$ and $q - \ell - 1$ have the common divisor ℓ. When ℓ is not prime, there are also divisors of the form $2^{\ell_i} - 1$, where $\ell_i|\ell$ and ℓ_i is prime. Suppose that q_i is a prime divisor of $2^{\ell_i} - 1$. Then $q_i = k_i \ell_i + 1$, and, since it is a factor of $2^\ell - 1$,

$$2^{\ell_i}(2^{q_i - \ell_i - 1} - 1) = 2^{q_i} - 1 \equiv 0 \ (mod\ q_i) \tag{3.2}$$

Since $\ell|(q-1)$, $\ell_i|(q-1)$ and $gcd(q_i - 1, q - 1) \geq \ell_i$. Therefore, $gcd(q_i - \ell_i - 1, q_i - 1) \geq \ell_i$ and the arithmetic sequence $n \equiv q_i - \ell_i - 1 \ (mod\ q_i - 1)$ has a nontrivial common factor.

The sequence $q - \ell - 1 \ (mod\ q - 1)$ also will consist of composite integers because $gcd(q - \ell - 1, q - 1) \geq \ell_i$. □

Proposition 2. The exponents of the form $k_1\varphi(n') + k_2\varphi(n'')$ consist of composite integers for $n',\ n'' \geq 3$. Then, if $2^n - 1 \equiv 0 \ (mod\ an' + bn')$ for any pair of integers $n',\ n'' \geq 3$, the exponent of the Mersenne number will be a composite integer. If n' or n'' equals 2, it cannot be determined from this congruence whether $2^n - 1$ is prime.

Proof. Suppose that the congruence of $2^n - 1$ is evaluated modulo a composite integer n'. Then

$$2^n - 1 \equiv 2^{n - k_1\varphi(n')} - 1 \qquad mod\ (n') \tag{3.3}$$

This integer can be reduced further modulo another composite number n''. Then

$$2^p - 1 \equiv 2^{p - k_1\varphi(n') - k_2\varphi(n'')} - 1 \qquad (mod\ an' + bn''). \tag{3.4}$$

if $n - k_1\varphi(n') - k_2\varphi(n'') = 0$. Unless $an' + bn''$ equals $2^n - 1$, this Mersenne number will be composite. If $gcd(n', n'') \neq 1$, then $\frac{an'+bn''}{gcd(n,n')} < an' + bn'' \leq 2^p - 1$, and $2^p - 1 \equiv 0 \ \left(mod \frac{an'+bn''}{gcd(n',n'')}\right)$. When $n' = p_1^{\alpha_1}...p_s^{\alpha_s}$ and $n'' = q_1^{\beta_1}...q_t^{\beta_t}$, $\varphi(n') = p_1^{\alpha_1 - 1}(p_1 - 1)...p_s^{\alpha_s - 1}(p_s - 1)$ and $\varphi(n'') = q_1^{\beta_1 - 1}(q_1 - 1)...q_t^{\beta_t - 1}(q_t - 1)$. Given that $gcd(n', n'') = 1$, the primes $\{p_i,\ i = 1, ..., s\}$ and $\{q_j,\ j =$

$1, ..., t\}$ can be chosen to be different. If n' and n'' are odd, $gcd(p_i - 1, q_j - 1) ge 2$ for the all of the odd prime factors p_i and q_j. Similarly, there is a nontrivial common factor of $2^{\alpha_i - 1}$ and $q_j - 1$ for $\alpha_i \geq 2$. Therefore, for these pairs of integers $gcd(\varphi(n'), \varphi(n'') \geq 2$ and $n = k_1\varphi(n') + k_2\varphi(n'')$ will be composite. When $n' = 2$, $gcd(\varphi(2), \varphi(n'') = 1$. However, $2^n - 1 \equiv 1 \ (mod\ 2)$ and it is necessary to choose $n'' = 1$ to have the congruence $2^n - 1 \equiv 0 \ (mod\ an' + bn'')$, and it cannot be determined whether $2^n - 1$ is prime. Again, for $n'' = 2$, $gcd(\varphi(n'), \varphi(2)) = 1$. Since $2^n - 1 \equiv 2^{n - k_1\varphi(n')} - 1 \ (mod\ n')$ and $2^{n - k_1\varphi(n')} - 1 \equiv 1 \ (mod\ an' + 2b)$, the divisibility of $2^n - 1$ cannot be concluded. □

Theorem 1. A probabilistic lower bound for the frequency of Mersenne numbers $2^p - 1$ is found such that the exponent p occurs in an arithmetical sequence with terms having a greatest common denominator equal to 1.

Proof. The congruence relations for $m^p - n$ can be considered modulo n', where n' is not a prime and $gcd(m, n') = 1$. For example, let $p \equiv \varphi(n') - \ell \ (mod\ \varphi(n'))$. Then

$$\begin{aligned} m^\ell(m^p - n) &\equiv m^\ell(m^{\varphi(n') - \ell} - n) && (mod\ n') \\ &= m^{\varphi(n')} - m^\ell \cdot n = 2^{\varphi(n')} - 2^\ell && (mod\ n') \\ &\equiv 1 - 2^\ell && (mod\ n'). \end{aligned} \tag{3.5}$$

Because all divisors of $2^\ell - 1$ are congruent to 1 modulo ℓ, let $n' = k\ell + 1$. With

$$p = k'\varphi(n') - \ell \tag{3.6}$$

and $gcd(\varphi(n'), \ell) = 1$, the arithmetic sequence in Eq.(3.6) would contain an infinite number of primes. Since

$$\varphi(k\ell + 1) = (k\ell + 1) \prod_i \frac{q_i - 1}{q_i} \tag{3.7}$$

where $q_i | (k\ell + 1)$. As $gcd(k\ell + 1, k) = gcd(k\ell + 1, \ell) = 1$, $gcd(q_i, k) = gcd(q_i, \ell) = 1$. It can be arranged also that there exists an infinite number of values of ℓ such that $gcd(q_i - 1, \ell) = 1$. If $\ell = \prod_\alpha \ell_\alpha$, $k\ell + 1$ can be rewritten as $k_\alpha \ell_\alpha + 1$ and the problem reduces to the existence of divisors of the form $\tilde{k}_\alpha \ell_\alpha + 1$. It follows that

$$y(\tilde{k}_\alpha \ell_\alpha + 1) = k_\alpha \ell_\alpha + 1 \tag{3.8}$$

for some integer y, which implies

$$y\tilde{k}_\alpha \ell_\alpha + y - 1 = k_\alpha \ell_\alpha \tag{3.9}$$

where

$$\begin{aligned} y - 1 &= x_\alpha \ell_\alpha \\ x_\alpha &\in \mathbb{Z}. \end{aligned} \tag{3.10}$$

When Eq.(3.10) holds, $gcd(y - 1, \ell_\alpha) = \ell_\alpha$ and $gcd(\varphi(n'), \ell) > 1$, since $y - 1$ can be identified

with $q_i - 1$ for some q_i. From Eq.(3.9),

$$y\tilde{k}_\alpha + x_\alpha = (1 + x_\alpha \ell_\alpha)\tilde{k}_\alpha + x_\alpha = k_\alpha \tag{3.11}$$

and

$$x_\alpha = \frac{k_\alpha - 1}{\tilde{k}_\alpha \ell_\alpha + 1} \tag{3.12}$$

As x_α must be integer, $(\tilde{k}_\alpha \ell_\alpha + 1)|(k_\alpha - 1)$ and the divisibility conditions for the compositenss of the sequence (3.6) are

$$\begin{aligned} \tilde{x}_\alpha | k_\alpha - 1 \\ \tilde{x}_\alpha | k_\alpha \ell_\alpha + 1 \end{aligned} \tag{3.13}$$

With $(k_\alpha \ell_\alpha + 1) - \ell_\alpha(k_\alpha - 1) = \ell_\alpha + 1$, there exists no solution to Eq.(3.13) if

$$gcd(k_\alpha - 1, \ell_\alpha + 1) = 1 \tag{3.14}$$

The frequency of integers k_α satisfying this constraint is bounded by

$$1 - \frac{(\tau(k_\alpha - 1) - 1)(\tau(\ell_\alpha + 1) - 1)}{min(\sqrt{k_\alpha - 1}, \sqrt{\ell_\alpha + 1})^2}$$

for $k_\alpha - 1 < \ell_\alpha + 1$, where $\tau(N)$ is the number of divisors of N. When $k_\alpha - 1 > \ell_\alpha + 1$, this frequency is repeated at intervals of $\ell_\alpha + 1$. Finally, ℓ_α may be allowed to vary to cover all possible values of ℓ. Based on these terms in the arithmetical sequence, the existence of an infinite number of primes follows from Dirichlet's theorem, with an additional periodic constraint in the character sums. □

There are implications, then, for the extent of the sequence of prime exponents such that $2^p - 1$ is composite. Although it might appear that the existence of a common divisor of $2^\ell - 1$ and $2^p - 1$ implies a composite nature of p, the validity of Eq.(3.5) actually provides the proof that this implication does not hold universally as primes do occur in the sequence (3.6) and this conclusion can be verified by the factorization tables [3].

4 Conclusion

The arithmetical sequences for the exponents of Mersenne numbers deduced from a geometrical representation of $2^n - 1$ appear to generate composite integers. In contrast with the method for $m^p - n$, where $m > 3$ and $n > 2$ and the arithmetical sequences for the exponents have initial terms and differences that are relatively prime, the corresponding sequences for $2^n - 1$ contained common factors regardless of the choice of the initial exponent. This technique can be modified by considering the congruence properties of $m^p - n$ modulo an integer n' which is not prime. Defining n' to be $k\ell + 1$, the sequence $k'\varphi(n') - \ell$ would contain an infinite number of primes if $gcd(\varphi(n'), \ell) = 1$ and Mersenne numbers with these exponents from this sequence are shown

to be divisible by n'. The frequency of this condition on $\varphi(n')$ being valid is shown to have a lower bound and therefore yields a probabilistic proof of the infinite extent of the sequence of composite Mersenne numbers with prime exponents.

Acknowledgements

The geometrical representation of the Mersenne number and several of the congruence conditions were obtained in research completed at the University of Sydney.

References

[1] Bang, A. S. Taltheoretische Undersogseler, *Tidsskrift for Mathematik*, Vol. 5, 1886, 70–80; 130–137.

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

[3] Brillhart, J., D. H. Lehmer, et. al., Factorizations of $b^n - 1$, $b = 2, 3, 5, 6, 7, 10.11.12$ up to high powers, *Cont. Math.*, Vol. 22, American Mathematical Society, Providence, 1983.

[4] Euler, L. Observationes De Theoremate Quodam Fermatiano Aliisque ad Numeros Primos Spectantibus, *Comm. Acad. Scientaiarum Petropolitanae*, Vol. 6, 1738, 103–107.

[5] Israel, R. B. Solution of Problem 6384, *Amer. Math. Monthly*, Vol. 90, 1983, 650.

[6] Indlekofer, K.-H., A. Járai, Largest Known Twin Primes and Sophie Germain Primes, *Math. Comp.*, Vol. 68, 1999, 1317–1324.

[7] Lagrange, J. L. *Recherches D'Arithmetique*, Nuov. Mém. Acad. Berlin, 1775, in Ouvres de Lagrange, Vol. 3, Gauthier-Villars, 1894, 695–795.

[8] Powell, B. Problem 6384, Numbers of the Form $m^p - n$, *Amer. Math. Monthly*, Vol. 89, 1982, 278.

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

[10] De la Rosa, B. Primes Powers and Partitions, *Fibonacci Quart.*, Vol. 16, 1978, No. 6, 518–522.

[11] Zsigmondy, K. Zur Theorie der Potenzreste, *Monatsh. Math.*, Vol. 3, 1892, 265–284.