Fermat and Mersenne Prime Criteria for the Infinity or the Strong finiteness of Primes of the Form $2^k \pm 1$

Pingyuan Zhou

E-mail：zhoupingyuan49@hotmail.com

Abstract

Gauss-Wantzel theorem is the first famous example in which Fermat primes are thought a criterion for the constructibility of regular polygons (though it does not include the constructibility of regular 2^k-sided polygons). It means that Fermat primes and Mersenne primes can separately become criteria for the infinity or the strong finiteness of primes of the form $2^x \pm 1$, which includes Fermat prime criteria for the set of Mersenne primes and its two subsets i. e. double Mersenne primes and root Mersemme primes as well as Mersenne prime criteria for the set of Fermat primes and its two subsets i.e. double Fermat primes and Catalan-type Fermat primes. In addition, such method can be generalized to understanding of the infinity of near-square primes of Mersenne primes by Fermat prime criterion. Thus we have some simple but clear criterion methods to handle the problems about the infinity or the strong finiteness of above kinds of primes arising from numbers of the form $2^x \pm 1$ but some of these problems have been known as very difficult ones such as Mersenne

primes to be conjectured as infinite but double Mersenne primes and Fermat primes to be conjectured as finite.

Keywords: Fermat prime croterion; Mersenne prime criterion; primes of the form $2^x \pm 1$; near-square prime of Mersenne prime; infinity; strong finiteness.

2010 Mathematics Subject Classification: 11A41, 11A51, 11A07, 51M04

1. Introduction

Well-known Gauss-Wantzel theorem states that a regular n-sided polygon is constructible with ruler and compass if and only if $n = 2^k p_1 p_2 ... p_t$ where k and t are non-negative integers, and each p_i is a (distinct) Fermat prime. In the theorem, Fermat primes are thought direct criterion for the constructibility of regular polygons in the following three cases: case for k=0 and t=1 to include all prime-sided constructible regular polygons (known number of such polygons is 5), case for k=0 and t=5 to include all odd-sided constructible regular polygons (known number of such polygons is 31) and case for $k \geq 1$ and t=5 to include all even-sided constructible regular polygons whose number of sides must contain a (distinct) Fermat prime(s) as odd prime factor(s) of number of sides (it is known that there is an infinite number of such polygons)[1]. Although by Gauss-Wantzel theorem the case for $k \geq 1$ and t=0 includes all even-sided constructible regular polygons whose number of sides is 2^k but is not related to Fermat primes, in our previous work[2] a finite sufficient condition has indirectly linked Fermat primes F_2, F_3, F_4 with the constructibility of regular 4-sided, 8-sided, 16-sides polygons to lead a generalized sufficient condition to link Fermat primes F_2, F_3, F_4 with the constructibility of all regular 2^k-sided polygons so that Fermat primes F_2, F_3, F_4 can be thought indirect criterion for the constructibility of all regular 2^k-sided polygons. These results make us fell Fermat primes also can become simple but clear criteria for other difficult problems such as the infinity of Mersenne primes and the finiteness of double Mersenne primes which have been conjectured for many years. Considering Fermat primes and Mersenne primes all arise from numbers of the form $2^x \pm 1$, it should be reasonable that Mersenne primes also can become simple but clear criteria for the finiteness of Fermat primes which is conjectured because any new Fermat prime has not been found since Fermat found such five primes. In general, Fermat primes can become criteria for the infinity or the strong finiteness of the set of Mersenne primes and its subsets but Mersenne primes can become criteria for the infinity or the strong finiteness of the set of Fermat primes and its subsets.

2. Fermat prime criterion for the infinity of Mersenne primes

Definition 2.1 If p is a prime number then $M_p=2^p-1$ is called a Mersenne number.

Definition 2.2 If Mersenne number $M_p=2^p-1$ is prime then the number M_p is called Mersenne prime.

Considering all Mersenne primes to arise from Mersenne numbers of the form $2^p–1$, we have the following definition.

Definition 2.3 All of primes are called basic sequence of number of Mersenne primes.

From Definition 2.3 we see basic sequence of number of Mersenne primes is an infinite sequence because prime numbers are infinite. Further we have the following definition.

Definition 2.4 If the first few continuous prime numbers p make $M_p=2^p–1$ become Mersenne primes in basic sequence of number of Mersenne primes then these prime numbers are called original continuous prime number sequence of Mersenne primes.

Lemma 2.1 The original continuous prime number sequence of Mersenne primes is p =2,3,5,7.

Proof. Since M_p for p = 2,3,5,7 are Mersenne primes but M_{11} is not Mersenne prime, by Definition 2.4 we can confirm there exists an original continuous prime number sequence of Mersenne primes i.e. p =2,3,5,7.

Definition 2.5 Mersenne primes are strongly finite if the first few continuous terms generated from the original continuous prime number sequence are prime but all larger terms are composite.

Fermat prime criterion 2.1 Mersenne primes are infinite if both the sum of corresponding original continuous prime number sequence and the first such prime are Fermat primes, but such primes are strongly finite if one of them is not Fermat prime.

Proposition 2.1 Mersenne primes are infinite.

Proof. Since the sum of original continuous prime number sequence of Mersenne primes i.e. 2+3+5+7=17 is a Fermat prime i.e. F_2 and the first Mersenne prime M_2=3 is a Fermat prime i.e. F_0, by Fermat prime criterion 2.1 Mersenne primes are infinite.

3. Fermat prime criterion for the strong finiteness of double Mersenne primes

Definition 3.1 If exponent of a Mersenne number is a Mersenne prime M_p i.e. $MM_p= 2^{M_p} -1$ then the Mersenne number MM_p is called double Mersenne number.

Definition 3.2 If a double Mersenne number $MM_p= 2^{M_p} -1$ is prime then the double Mersenne number MM_p is called double Mersenne prime.

Considering all double Mersenne primes to arise from double Mersenne numbers of the form $2^{M_p} -1$, we have the following definition.

Definition 3.3 Exponents of all Mersenne primes M_p are called basic sequence of number of doube Mersenne primes.

From Definition 3.3 we see basic sequence of number of double Mersenne primes is an infinite sequence if Mersenne primes are infinite. Lenstra, Pomerance and Wagstaff have conjectured that there is an infinite number of Mersenne primes in studying the number of primes p less than x with $2^p–1$ being prime[3]. Our above argument also presents the same result i. e. Mersenne primes are infinite. Thus by Definition 3.3 basic sequence of number of double Mersenne primes is an infinite sequence. Further we have the following definition.

Definition 3.4 If the first few continuous exponents p of Mersenne primes M_p make double Mersenne number $MM_p = 2^{M_p} - 1$ become double Mersenne primes in basic sequence of number of double Mersenne primes then these exponents p of Mersenne primes are called original continuous prime number sequence of double Mersenne primes.

Lemma 3.1 The original continuous prime number sequence of double Mersenne primes is p =2,3,5,7.

Proof. Since MM_p for p = 2,3,5,7 are known double Mersenne primes but MM_{13} is not double Mersenne prime because of existence of known factors for MM_{13}[4], by Definition 3.4 we can confirm there exists an original continuous prime number sequence of double Mersenne primes i.e. p =2,3,5,7.

Definition 3.5 Double Mersenne primes are strongly finite if the first few continuous terms generated from the original continuous prime number sequence are prime but all larger terms are composite.

Fermat prime criterion 3.1 Double Mersenne primes are infinite if both the sum of corresponding original continuous prime number sequence and the first such prime are Fermat primes, but such primes are strongly finite if one of them is not Fermat prime.

Proposition 3.1 Double Mersenne primes are strongly finite.

Proof. Since the sum of original continuous prime number sequence of double Mersenne primes i.e. 2+3+5+7=17 is a Fermat prime i.e. F_2 but the first double Mersenne prime MM_2=7 is not a Fermat prime, by Fermat prime criterion 3.1 double Mersenne primes are strongly finite.

Proposition 3.1 means that double Mersenne primes are strongly finite, that is, every double Mersenne number MM_p is composite for p >7.

Proposition 3.2 MM_{127} and all of the following terms are composite in Catalan-Mersenne number sequence.

Proof. By Lemma 3.1, Definition 3.5 and Proposition 3.1 we see every double Mersenne number MM_p is composite for p >7. Since 127>7, MM_{127} is composite so that all of the following terms are composite in Catalan-Mersenne number sequence[5].

Proposition 3.3 There are infinitely many composite Mersenne numbers.

Proof. By Proposition 2.1 there are infinitely many Mersenne primes M_p. Then by Definition 3.1 there are infinitely many double Mersenne numbers MM_p. By Lemma 3.1, Definition 3.5 and Proposition 3.1 we see every double Mersenne number MM_p is composite for p >7. Thus there are infinitely many composite double Mersenne numbers MM_p. Since every double Mersenne number is also a Mersenne number by Definition 2.1, Definition 2.2 and Definition 3.1, every composite double Mersenne number is also a composite Mersenne numbers. Hence there are infinitely many composite Mersenne numbers.

Remark 3.1 Euler showed a theorem: If k > 1 and $p = 4k+3$ is prime, then $2p+1$ is prime if and only if $2^p \equiv 1(\bmod 2p+1)$[6]. It implies that if both $p = 4k+3$ and $2p+1$ are prime then Mersenne number 2^p-1 is composite because $2p+1$ is a prime factor of

2^p-1 from the theorem, which means if there are infinitely many prime pairs (p, $2p+1$) for $p = 4k+3$ then there are infinitely many composite Mersenne numbers. But it has not been a solved problem because the existence of infinitely many prime pairs (p, $2p+1$) for $p = 4k+3$ has not been proven.

4. Fermat prime criterion for the infinity of root Mersenne primes

Definition 4.1. Mersenne primes M_p for p=2,3,5,7 and Mersenne primes M_p to satisfy congruences $p \equiv F_0 \pmod 8$ or $p \equiv F_1 \pmod 6$ are called root Mersenne primes, where $F_0 = 3$ and $F_1 = 5$ are Fermat primes[7,8,9].

Although every one of p=2,3,5,7 is too small to be considered whether satisfy congruences $p \equiv F_0 \pmod 8$ or $p \equiv F_1 \pmod 6$, their sum 2+3+5+7=17 satisfies congruence $17 \equiv 5 \pmod 6$ so that M_p for p=2,3,5,7 are thought root Mersenne primes[7]. Obviously, root Mersenne primes are a subset of Mersenne primes.

By Definition 4.1 we see that among 48 known Mersenne primes, there are 31 known root Mersenne primes: M_2, M_3, M_5, M_7, M_{17}, M_{19}, M_{89}, M_{107}, M_{521}, M_{2203}, M_{4253}, M_{9689}, M_{9941}, M_{11213}, M_{19937}, M_{21701}, M_{86243}, M_{216091}, M_{756839}, M_{859433}, $M_{1257787}$, $M_{1398269}$, $M_{2976221}$, $M_{3021377}$, $M_{6972593}$, $M_{20996011}$, $M_{25964951}$, $M_{32582657}$, $M_{37156667}$, $M_{43112609}$, $M_{57885161}$. Hence we have the following proposition.

Proposition 4.1. Let F_k be Fermat primes, then the number of root Mersenne primes M_p is 2^k for $p<F_k$.

Proof. For Proposition 4.1, we have the following verification.

For k=0, there exists 2^0=1 root Mersenne prime i.e. M_2 for $p<F_0$ i.e. $p<3$;

For k=1, there exist 2^1=2 root Mersenne primes i.e. M_2, M_3 for $p<F_1$ i.e. $p<5$;

For k=2, there exist 2^2=4 root Mersenne primes i.e. M_2, M_3, M_5, M_7 for $p<F_2$ i.e. $p<17$;

For k=3, there exist 2^3=8 root Mersenne primes i.e. M_2, M_3, M_5, M_7, M_{17}, M_{19}, M_{89}, M_{107} for $p<F_3$ i.e. $p<257$;

For k=4, there exist 2^4=16 root Mersenne primes i.e. M_2, M_3, M_5, M_7, M_{17}, M_{19}, M_{89}, M_{107}, M_{521}, M_{2203}, M_{4253}, M_{9689}, M_{9941}, M_{11213}, M_{19937}, M_{21701} for $p<F_4$ i.e. $p<65537$.

Since it is known that there exist no any undiscovered Mersenne primes M_p for $p \leq 30402457$[11], which means there exist no any undiscovered root Mersenne primes for $p \leq 30402457$, and all Fermat numbers F_k are composite for $5 \leq k \leq 32$ and there is no any found new Fermat prime for $k>4$[12], if suppose every Fermat number F_k is composite for $k>4$ then Proposition 4.1 holds.

Considering all root Mersenne primes to arise from Mersenne primes, we have the following definition.

Definition 4.2. Exponents p of all Mersenne primes M_p are called basic sequence of number of root Mersenne primes.

From Definition 4.2 we see that basic sequence of number of root Mersenne primes is an infinite sequence if Mersenne primes are infinite. Further we have the following definition.

Definition 4.3. If the first few continuous exponents of Mersenne primes p make $M_p=2^p-1$ become root Mersenne primes in basic sequence of number of root Mersenne primes then these exponents are called original continuous prime number sequence of root Mersenne primes.

Lemma 4.1. The original continuous prime number sequence of root Mersenne primes is p =2,3,5,7.

Proof. Since M_p for p = 2,3,5,7 are root Mersenne primes but Mersenne prime M_{13} is not root Mersenne prime, by Definition 4.3 we can confirm there exists an original continuous prime number sequence of root Mersenne primes i.e. p =2,3,5,7.

Definition 4.4. Root Mersenne primes are strongly finite if the first few continuous terms generated from the original continuous prime number sequence are prime but all larger terms are composite.

Fermat prime criterion 4.1 Root Mersenne primes are infinite if both the sum of corresponding original continuous prime number sequence and the first such prime are Fermat primes, but such primes are strongly finite if one of them is not Fermat prime.

Propposition 4.2 Root Mersenne primes are infinite.

Proof. Since the sum of original continuous prime number sequence of root Mersenne primes i.e. 2+3+5+7=17 is a Fermat prime i.e. F_2 and the first root Mersenne prime M_2=3 is also a Fermat prime i.e. F_0, by Fermat prime criterion 4.1 root Mersenne primes are infinite.

From above argument we see root Mersenne primes are infinite but the first finite number of root Mersenne primes (from M_2 to M_{21701}) present finite but positive distribution law as Proposition 4.1 shows. It means that we have a finite sufficient condition for the constructibility of regular 2^k-sided polygons.

Finite sufficient condition 4.1 An even-sided regular polygon can be constructed with compass and straightedge if the number of sides is the number 2^k of root Mersenne primes M_p for $p<F_k$ being Fermat primes when $2\le k\le 4$.

By Proposition 4.1 the condition holds, that is, F_2, F_3, F_4 are indirect criterion for the constructibility of regular 4-sided polygon, regular 8-sided polygon, regular 16-sided polygon. It means that existence of Fermat primes F_2, F_3, F_4 will lead regular 4-sided polygon, regular 8-sided polygon, regular 16-sided polygon to be constructible with compass and straightedge. Hence we have the following generalized sufficient condition.

Generalized sufficient condition 4.1 An even-sided regular polygon can be constructed with compass and straightedge if the number of sides is 2^k being a generalization of the number of root Mersenne primes M_p for $p<F_k$ being Fermat primes when $2\leq k\leq 4$.

If the generalized sufficient condition is acceptable then every case showed by Gauss-Wantzel theorem will imply existence of direct or indirect connections between Fermat primes and all constructible regular polygons. It means that definition of root Mersenne primes are reasonable because the finite distribution law of root Mersenne primes are positive as Preposition 4.1 shows, which will make Gauss-Wantzel theorem have general sense in implying existence of connections between Fermat primes and all constructible regular polygons.

5. Fermat prime criterion for the infinity of near-square primes of Mersenne primes

Above argument considered the set of Mersenne primes and its two subsets but such Fermat prime criterion method will be generalized to a kind of near-square primes of Mersenne primes M_p i.e. primes of the form $2M_p^2-1$.

The traditional relation formula between perfect number P_p and Mersenne prime M_p can be expressed as

$$P_p = (M_p^2 + M_p)/2. \qquad (1)$$

From (1) we have

$$W_p = 2(2P_p–M_p) –1, \qquad (2)$$

where

$$W_p = 2M_p^2 –1 \qquad (3)$$

is a near-square number of Mersenne prime M_p, so that there is a near-square number sequence $W_p = 2M_p^2 –1$ generated from all Mersenne primes M_p. If Mersenne primes M_p are infinite then $W_p = 2M_p^2 –1$ is an infinite sequence. From $M_p=2^p–1$ we get structure of near-square number $W_p = 2M_p^2 –1$ as follows

$$W_p = 2^{2p+1}–2^{p+2}+1, \qquad (4)$$

where p is exponent of Mersenne prime $M_p=2^p–1$. Hence we have the following definition.

Definition 5.1 If M_p is a Mersenne prime then $W_p = 2M_p^2 –1$ is called near-square number of Mersenne prime M_p**.**

By Proposition 2.1 Mersenne primes are infinite, so near-square numbers of Mersenne primes M_p are an infinite sequence.

Definition 5.2 If a near-square number $W_p = 2M_p^2 –1$ of Mersenne prime M_p is prime then W_p is called near-square prime of Mersenne prime M_p**.**

Considering near-square primes of Mersenne primes to arise from the near-square numbers $W_p = 2M_p^2 - 1$ which are an infinite sequence, we have the following definition.

Definition 5.3. Exponents p of all Mersenne primes M_p are called basic sequence of number of near-square primes of Mersenne primes M_p**.**

It is obvious that we can not consider every near-square number W_p of Mersenne prime M_p to be a prime number. In this near-square number sequence, we have verified the first few prime terms as follows[7]

$W_2=2^5-2^4+1=17$,

$W_3=2^7-2^5+1=97$,

$W_7=2^{15}-2^9+1=32257$,

$W_{17}=2^{35}-2^{19}+1=34359214081$

$W_{19}=2^{39}-2^{21}+1=549753716737$

…

From (2) we see every prime W_p is larger than corresponding perfect number $P_p = (M_p^2 + M_p)/2$.

Definition 5.4. If the first few continuous exponents of Mersenne primes p make $W_p = 2M_p^2 - 1$ become near-square primes of Mersenne primes in basic sequence of number of near-square primes of Mersenne primes then these exponents are called original continuous prime number sequence of near-square primes of Mersenne primes.

Lemma 5.1. The original continuous prime number sequence of near-square primes of Mersenne primes is p =2,3.

Proof. Since the first two near-square numbers of Mersenne primes i.e. W_2=17 and W_3=97 all are near-square primes of Mersenne primes but the third near-square number of Mersenne prime M_5 i.e. W_5=1921 is composite, by Definition 5.4 the original continuous prime number sequence of near-square primes of Mersenne primes is p =2,3.

Definition 5.5 Near-square primes of Mersenne primes are strongly finite if the first few continuous terms generated from the original continuous prime number sequence are prime but all larger terms are composite.

Fermat prime criterion 5.1. Near-square primes of Mersenne primes are infinite if both the sum of corresponding original continuous prime number sequence and the first such prime are Fermat primes, but such primes are strongly finite if one of them is not Fermat prime.

Proposition 5.1 Near-square primes of Mersenne are infinite.

Proof. Since the sum of original continuous prime number sequence of near-square primes of Mersenne primes i.e. 2+3=5 is a Fermat prime i.e. F_1 and the first near-square prime of Mersenne prime W_2=17 is also a Fermat prime i.e. F_2, by Fermat prime criterion 5.1 near-square primes of Mersenne are infinite.

Obviously, Proposition 5.1 will support our previous result i. e. larger primes than the most largest known Mersenne prime may be found from near-square numbers of known Mersenne primes with large *p*-values[7].

6. Mersenne prime criterion for the strong finiteness of Fermat primes

Definition 6.1 If n is a natural number (n = 0,1,2,3, …) then $F_n = 2^{2^n} +1$ is called a Fermat number.

Definition 6.2 If Fermat number $F_n = 2^{2^n} +1$ is prime then the Fermat number F_n is called Fermat prime.

Considering all Fermat primes to arise from Fermat numbers of the form $2^{2^n} +1$, we have the following definition.

Definition 6.3 All of natural numbers are called basic sequence of number of Fermat primes.

From Definition 6.3 we see basic sequence of number of Fermat primes is an infinite sequence because natural numbers are infinite. Further we have the following definition.

Definition 6.4 If the first few continuous natural numbers *n* make $F_n = 2^{2^n} + 1$ become Fermat primes in basic sequence of number of Fermat primes then these natural numbers are called original continuous natural number sequence of Fermat primes.

Lemma 6.1 The original continuous natural number sequence of Fermat primes is n = 0,1,2,3,4.

Proof. Since F_n for n = 0,1,2,3,4 are Fermat primes but F_5 is not Fermat prime, by Definition 6.4 we can confirm there exists an original continuous natural number sequence of Fermat primes i.e. n = 0,1,2,3,4.

Definition 6.5 Fermat primes are strongly finite if the first few continuous terms generated from the original continuous natural number sequence are prime but all larger terms are composite.

Mersenne prime criterion 6.1 Fermat primes are infinite if both the sum of corresponding original continuous natural number sequence and the first such prime are Mersenne primes, but such primes are strongly finite if one of them is not Mersenne prime.

Proposition 6.1 Fermat primes are strongly finite.

Proof. Since the first Fermat prime $F_0=3$ is a Mersenne prime i.e. M_2 but the sum of original continuous natural number sequence of Fermat primes i.e. 0+1+2+3+4=10 is not a Mersenne prime, by Mersenne prime criterion 6.1 Fermat primes are strongly finite.

By Lemma 6.1 and Proposition 6.1 we see every Fermat number F_n are composite for $n>4$. The result will support Proposition 4.1 to hold so that we believe Gauss-Wantzel theorem can imply existence of general connections between Fermat primes and all constructible regular polygons, and the following open problem about Fermat numbers will be solved.

Proposition 6.2 There are infinitely many composite Fermat numbers.

Proof. By Propposition 6.1 Fermat primes are strongly finite but Fermat numbers are infinite, hence composite Fermat numbers are infinite.

Remark 6.1 In order to solve the problem, there is a conjecture that if F_n is composite then F_{n+1} is composite. However, there has not appeared any argument about the conjecture.

Proposition 6.3 There are infinitely many composite numbers of the form x^2+1.

Proof. Since there are recurrence relation of Fermat numbers i.e. $F_{n+1}=(F_n-1)^2+1$ for $n\geq0$ and Fermat numbers $F_{n+1}=(F_n-1)^2+1$ are a subset of numbers of the form x^2+1 and by Proposition 6.2 there are infinitely many composite Fermat numbers. Hence composite numbers of the form x^2+1 are infinite.

7. Mersenne prime criterion for the strong finiteness of double Fermat primes

Double Fermat numbers[8,10] are a subset of Fermat numbers, so double Fermat primes are a subset of Fermat primes. By Proposition 6.1 Fermat primes are strongly finite i.e. there are only 5 Fermat primes $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$, thus the existence of double Fermat primes greater than 65537 is not allowed.

Definition 7.1 If F_n is a Fermat number then $F_{2^n}=2^{F_n-1}+1$ is called a double Fermat number.

Double Fermat numbers F_{2^n} is a subset of the set of Fermat numbers F_n and satisfy the recurrence relations $F_{2^{n+1}} = (F_{2^n} - 1)^{F_n - 1} + 1$ with F_{2^0} =5 for $n \geq 0$[8].

Definition 7.2 If double Fermat number $F_{2^n} = 2^{F_n - 1} + 1$ is prime then the double Fermat number F_{2^n} is called double Fermat prime.

Considering all double Fermat primes to arise from double Fermat numbers of the form $2^{F_n - 1} + 1$, we have the following definition.

Definition 7.3 All of natural numbers are called basic sequence of number of double Fermat primes.

From Definition 7.3 we see basic sequence of number of double Fermat primes is an infinite sequence because natural numbers are infinite. Further we have the following definition.

Definition 7.4 If the first few continuous natural numbers n make $2^{F_n - 1} + 1$ become double Fermat primes in basic sequence of number of double Fermat primes then these natural numbers are called original continuous natural number sequence of double Fermat primes.

Lemma 7.1 The original continuous natural number sequence of double Fermat primes is n = 0,1,2.

Proof. Since the first three double Fermat numbers F_{2^n} for n=0,1,2 i.e. F_{2^0} =5, F_{2^1} =17, F_{2^2} =65537 are double Fermat primes but the third double Fermat number $F_{2^3} = 2^{F_3 - 1}$ +1=F_8 is not double Fermat prime, by Definition 7.4 we can confirm there exists an original continuous natural number sequence of double Fermat primes i.e. n = 0,1,2.

Definition 7.5 Double Fermat primes are strongly finite if the first few continuous terms generated from the original continuous natural number sequence are prime but all larger terms are composite.

Mersenne prime criterion 7.1 Double Fermat primes are infinite if both the sum of corresponding original continuous natural number sequence and the first such prime are Mersenne primes, but such primes are strongly finite if one of them is not Mersenne prime.

Proposition 7.1 Double Fermat primes are strongly finite.

Proof. Since sum of original continuous natural number sequence of double Fermat primes i.e. 0+1+2=3 is a Mersenne prime i.e. M_2=3 but the first double Fermat prime F_{2^0} = 5 is not a Mersenne prime, by Mersenne prime criterion 7.1 double Fermat primes are strongly finite.

By lemma 7.1, Definition 7.5 and Proposition 7.1 we know there are only three double Fermat primes $F_{2^0}=5$, $F_{2^1}=17$, $F_{2^2}=65537$.

Proposition 7.2 There are infinitely many composite double Fermat numbers.

Proof. By Proposition 7.1 double Fermat primes are strongly finite but double Fermat numbers are infinite, hence composite double Fermat numbers are infinite.

Proposition 7.3 Fermat's little theorem for Fermat numbers has an equivalent statement $F_m \equiv 2 \pmod{F_n}$, where $m = 2^n$.

Poof. Fermat's little theorem for Fermat numbers is written $2^{F_n-1} \equiv 1 \pmod{F_n}$ in general since every F_n is co-prime to base 2. When double Fermat number formula $F_{2^n} = 2^{F_n-1}+1$ is introduced, $2^{F_n-1} \equiv 1 \pmod{F_n}$ becomes $F_{2^n} \equiv 2 \pmod{F_n}$. Le $m = 2^n$, we obtain $F_m \equiv 2 \pmod{F_n}$ which is an equivalent statement of Fermat's little theorem for Fermat numbers.

Remark 7.1 Proposition 7.3 just presents the property involving Fermat numbers that F_n–2 is divisible by all smaller Fermat numbers since $m = 2^n > n$.

8. Mersenne prime criterion for the strong finiteness of Catalan-type Fermat primes

Catalan-type Fermat numbers[10] are a subset of Fermat numbers, so Catalan-type Fermat primes are a subset of Fermat primes. By Proposition 6.1 Fermat primes are strongly finite i.e. there are only 5 Fermat primes F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537, thus the existence of Catalan-type Fermat primes greater than 65537 is not allowed.

Definition 8.1 Fermat numbers $F_c(n)$, which satisfy the recurrence relations $F_c(n+1) = 2^{F_c(n)-1}+1$ with $F_c(0) = F_0 = 3$ for $n \geq 0$, are called Catalan-type Fermat numbers.

An anonymous writer proposed that such numbers were all prime, however, this conjecture was refuted when Selfridge showed F_{16} is composite in 1953[11]. Catalan-type Fermat numbers are infinite and grow very quickly:

$F_c(0) = F_0 = 3$

$F_c(1) = 2^{F_c(0)-1}+1 = F_{2^0} = F_1 = 5$

$F_c(2) = 2^{F_c(1)-1}+1 = F_{2^1} = F_2 = 17$

$F_c(3) = 2^{F_c(2)-1}+1 = F_{2^2} = F_4 = 65537$

$F_c(4) = 2^{F_c(3)-1}+1 = F_{2^4} = F_{16} = 2^{65536}+1$

$F_c(5) = 2^{F_c(4)-1}+1 = F_{2^{16}} = F_{65536}$

$F_c(6) = 2^{F_c(5)-1}+1 = F_{2^{65536}}$

…

Catalan-type Fermat numbers are another subset of the set of Fermat numbers but are not a subsequence of double Fermat numbers since the first Catalan-type Fermat number $F_c\,(0) = F_0$ is a Fermat number but is not a double Fermat number though $F_c\,(1)$ and all of the following Catalan-type Fermat numbers are double Fermat numbers.

Definition 8.2 If Catalan-type Fermat number $F_c\,(n)$ is prime then the Catalan-type Fermat number $F_c\,(n)$ is called Catalan-type Fermat prime.

Considering all Catalan-type Fermat primes to arise from Catalan-type Fermat numbers generated from the recurrence relations $F_c\,(n+1) = 2^{F_c(n)-1} + 1$ with $F_c\,(0) = F_0 = 3$ for $n \geq 0$, we have the following definition.

Definition 8.3 All of natural numbers are called basic sequence of number of Catalan-type Fermat primes.

From Definition 8.3 we see basic sequence of number of Catalan-type Fermat primes is an infinite sequence because natural numbers are infinite. Further we have the following definition.

Definition 8.4 If the first few continuous natural numbers n make $F_c\,(n)$ become Catalan-type Fermat primes in basic sequence of number of Catalan-type Fermat primes then these natural numbers are called original continuous natural number sequence of Catalan-type Fermat primes.

Lemma 8.1 The original continuous natural number sequence of Catalan-type Fermat primes is $n = 0,1,2,3$.

Proof. Since the first four Catalan-type Fermat numbers $F_c(n)$ for n=0,1,2,3 i.e. $F_c(0) = 3$, $F_c(1) = 5$, $F_c(2) = 17$, $F_c(3) = 65537$ are Catalan-type Fermat primes but $F_c(4) = F_{16}$ is not Catalan-type Fermat prime, by Definition 8.4 we can confirm there exists an original continuous natural number sequence of Catalan-type Fermat primes i.e. $n = 0,1,2,3$.

Definition 8.5 Catalan-type Fermat primes are strongly finite if the first few continuous terms generated from the original continuous natural number sequence are prime but all larger terms are composite.

Mersenne prime criterion 8.1 Catalan-type Fermat primes are infinite if both the sum of corresponding original continuous natural number sequence and the first such prime are Mersenne primes, but such primes are strongly finite if one of them is not Mersenne prime.

Proposition 8.1 Catalan-type Fermat primes are strongly finite.

Proof. Since the first Catalan-type Fermat prime $F_c(0) = 3$ is a Mersenne prime i.e. M_2=3 but the sum of original continuous natural number sequence of Catalan-type

Fermat primes i.e. 0+1+2+3=6 is not a Mersenne prime, by Mersenne prime criterion 8.1 Catalan-type Fermat primes are strongly finite.

Proposition 8.2 There are infinitely many composite Catalan-type Fermat numbers.

Proof. By Proposition 8.1 Catalan-type Fermat primes are strongly finite but Catalan-type Fermat numbers are infinite, hence composite Catalan-type Fermat numbers are infinite.

9. Conclusions

In this paper, our arguments about Fermat prime criteria for the infinity of Mersenne primes, root Mersenne primes and near-square primes of Mersenne primes and the strong finiteness of double Mersenne primes and Mersenne prime criteria for the strong finiteness of Fermat, double Fermat and Catalan-type Fermat primes make it become possible that we may use very simple and clear criterion methods to give elementary results for problems about infinity and finiteness of prime number sequences generating from numbers of the form $2^x \pm 1$ (Fermat prime criterion for the infinity of near-square primes of Mersenne primes is a generalization here). In the mathematical frame, all results are elementary but seem to be natural and logically identical, which include all additional propositions such as Catalan-Mersenne number MM_{127} to be composite, existence of infinitely many composite Mersenne numbers, the number of root Mersenne primes for p less than Fermat primes to make

Gauss-Wantzel theorem have general sense in implying existence of direct or indirect connections between Fermat primes and constructible regular polygons, existence of infinitely many composite Fermat numbers, an equivalent statement of Fermat's little theorem for Fermat numbers to present the property involving Fermat numbers that F_n–2 is divisible by all smaller Fermat numbers because of $m = 2^n > n$, and so on. From these discussions we see it should be acceptable that if Fermat and Mersenne prime criterion methods are introduced in this mathematical frame then we will get some elementary but very simple and direct results for many very difficult problems.

References

[1]. Constructible polygon in The On-Line Wikipedia.
http://en.wikipedia.org/wiki/Constructible_polygon

[2]. Pingyuan Zhou, Fermat Primes to Become Criterion for the Constructibility of Regular 2^k-sided Polygons in The On-Line viXra
http://vixra.org/pdf/1407.0209v1.pdf

[3]. Mersenne conjectures in The On-Line Wikipedia.
http://en.wikipedia.org/wiki/Mersenne_conjectures

[4]. Double Mersenne Number in The On-Line Wolfram MathWorld.
http://mathworld.wolfram.com/DoubleMersenneNumber.html

[5]. Double Mersenne number in The On-Line Wikipedia.
http://en.wikipedia.org/wiki/Double_Mersenne_number

[6]. Mersenne Primes: History, Theorems and Lists in The On-Line Prime Pages.
http://primes.utm.edu/mersenne/

[7]. Pingyuan Zhou, Distribution and Application of Root Mersenne Prime, Global Journal of Mathematical Sciences: Theory and Practical, Vol.3, No.2(2011), 137-142.
http://www.irphouse.com/gjms/GJMSv3n2_4.pdf

[8]. Pingyuan Zhou, On the Connections between Mersenne and Fermat Primes, Glob. J. Pure Appl. Math. Vol.8, No.4(2012),453-458. Full text is available at EBSCO-ASC accession 86232958.
http://connection.ebscohost.com/c/articles/86232958/connections-between-mersenne-fermat-primes

[9]. Pingyuan Zhou, On the Existence of Infinitely Many Primes of the Form x^2+1, Glob. J. Pure Appl. Math. Vol.8, No.2(2012), 161-166. Full text is available at EBSCO-ASC accession 86233920.
http://connection.ebscohost.com/c/articles/86233920/existence-infinitely-many-primes

[10]. Pingyuan Zhou, Catalan-type Fermat Numbers, Glob. J. Pure Appl. Math. Vol.8, No.5(2012),579-582. Full text is available at EBSCO-ASC accession 86232974.
http://connection.ebscohost.com/c/articles/86232974/catalan-type-fermat-number

[11]. Fermat Number in The On-Line Wolfram MathWorld.
http://mathworld.wolfram.com/FermatNumber.html