Fermat Primes to Become Criterion for the Constructibility of Regular 2^k-sided Polygons

Pingyuan Zhou

E-mail：zhoupingyuan49@hotmail.com

Abstract

Gauss-Wantzel theorem shows that regular *n*-sided polygons, whose number of sides contains a (distrinct) Fermat prime(s) as odd prime factor(s) of *n* or number of sides is power of 2, are all constructible with compass and straightedge. But of these cases, the constructibility of all regular 2^k-sided polygons is not related to Fermat primes. We discover the number of so-called root Mersenne primes M_p for $p<F_k$ being Fermat primes is just 2^k for $2\leq k\leq 4$ so that the constructibility of regular 4-sided, 8-sided and 16-sided polygons can be indirectly explained by existence of Fermat primes. If it can be generalize to case for $k>4$ (though there are no known Fermat primes F_k for $k>4$) then the constructibility of all regular 2^k-sided polygons can be indirectly explained by Fermat primes as criterion. Thus there exist direct or indirect connections between Fermat primes and all constructible regular polygons according to the theorem.

Keywords: Fermat prime; Gauss-Wantzel theorem; the number of root Mersenne primes; constructibility of regular 2^k-sided polygon.

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

1. Gauss-Wantzel theorem

Which regular polygons are constructible? It had been a famous and open problem for more 2000 years before Gauss proved the constructibility of the regular 17-sided polygon in 1796. After the well-known discovery in geometry, Gauss developed the theory of Gaussian periods in his Disquistiones Arithmeticae. The theory allowed him to formulate a sufficient condition for the constructibility of regular polygons in 1801: A regular n-sided polygon can be constructed with compass and straightedge if n is power of 2 or the product of a power of 2 and any number of distinct Fermat primes. This is an important result in searching for connections between Fermat primes and geometry problems. In 1837, a full proof of necessity was given by Pierre Wantzel and the result is known as the Gauss-Wantzel theorem[1].

Theorem 1.1 (Gauss-Wantzel theorem). 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.

Case 1.1 (Theorem1.1). For k=0 and t=1, there are 5 prime-sided regular polygons to be constructible with compass and straightedge since there are 5 known Fermat primes i.e. F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537 to lead the number of sides to be 3,5,17,257,65537. If suppose Fermat number F_m is composite for all m>4 then there are only 5 prime-sided regular polygons to be constructible. In this case, Fermat

primes are the most direct and obvious criterion for the constructibility of prime-sided regular polygons.

Case 1.2 (Theorem 1.1). For k=0 and t=5, by Gauss-Wantzel theorem there are 31 odd-sided regular polygons to be constructible with compass and straightedge since there are 5 known Fermat primes i.e. F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537 to lead the number of sides to be 3, 5, 15, 17, 51, 85, 255, 257, 771, 1285, 3855, 4369, 13107, 21845, 65535, 65537, 196611, 327685, 983055, 1114129, 3342387, 5570645, 16711935, 16843009, 50529027, 84215045, 252645135, 286331153, 858993459, 1431655765, 4294967295[2]. If suppose Fermat number F_m is composite for all m>4 then there are only 31 odd-sided regular polygons to be constructible. In this case, Fermat primes are the most direct and obvious criterion for the constructibility of odd-sided regular polygons.

Case 1.3 (Theorem 1.1). For $k\geq1$ and t=5, by Gauss-Wantzel theorem there is an infinite number of even-sided regular polygons to be constructible with compass and straightedge though there are only 5 known Fermat primes, and the number of sides must contain a (distrinct) Fermat prime(s) as odd prime factor(s) of the number of sides for any considered even-sided regular polygon and the number of sides is 6,10,12,20,24,30,34,40,48,60,68,80,96,102,120,…[3]. In this case, Fermat primes are direct criterion for the constructibility of even-sided regular polygons.

Case 1.4 (Theorem1.1). For $k \geq 1$ and $t=0$, by Gauss-Wantzel theorem there is an infinite number of even-sided regular polygons to be constructible with compass and straightedge, whose number of sides is power of 2 and is not related to Fermat primes. The number of sides of regular 2^k-sided polygons is 4,8,16,32,64,128,256,512,…[3]. In this case, Fermat primes are not criterion for the constructibility of even-sided regular polygons.

By Gauss-Wantzel theorem Case 1.1, Case 1.2 and Case 1.3 completely present direct connections between Fermat primes and the constructibility of regular polygons but Case1.4 implies the constructibility of all regular 2^k-sided polygons is not related to Fermat primes, in other words, Fermat primes are not criterion for the constructibility of such an infinite number of even-sided regular polygons. However, studying for the number of so-called root Mersenne primes M_p for $p<F_k$ being Fermat primes is possibly useful for finding indirect connections between Fermat primes and the constructibility of all regular 2^k-sided polygons to present every case showed by Gauss-Wantzel theorem to imply existence of connections between Fermat primes and constructible regular polygons.

2. The number of root Mersenne primes M_p for $p< F_k$

Definition 2.1 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[4,5,6].

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[4]. Obviously, root Mersenne primes are a subset of Mersenne primes.

By Definition 2.1 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}, $M_{1257787}$, $M_{1398269}$, $M_{2976221}$, $M_{3021377}$, $M_{6972593}$, $M_{20996011}$, $M_{25964951}$, $M_{32582657}$, $M_{37156667}$, $M_{43112609}$ and $M_{57885161.}$ Hence we have the following proposition.

Proposition 2.1 Let F_k be Fermat primes for $k \geq 1$, then the number of root Mersenne primes M_p is 2^k for $p<F_k$.

Proof. Since the intersection of the set of Mersenne primes and the set of Fermat primes is a set to contain only one element 3, there is no any Fermat prime greater than 3 is also a Mersenne prime. It means there is no any Fermat prime greater than 3 is also a root Mersenne prime. Thus for Proposition 2.1, we have the following verification.

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 $p \leq 30402457$[7] and all Fermat numbers F_k are composite for $5 \leq k \leq 32$ and there is no any found new Fermat prime for $k>4$, if suppose every Fermat number F_k is composite for $k>4$ then Proposition 2.1 holds.

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

Definition 2.2 Exponents p of all Mersenne primes M_p are called basic sequence of number of root Mersenne primes.

From Definition 2.2 we see basic sequence of number of root Mersenne primes is an infinite sequence if Mersenne primes are infinite. Further we have the following definition.

Definition 2.3 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 2.1 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 2.3 we can confirm there exists an original continuous prime number sequence of root Mersenne primes i.e. p =2,3,5,7.

Definition 2.4 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.

Hence we have the following Fermat prime criterion.

Fermat prime criterion 2.1 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.

Corollary 2.1 If Fermat prime criterion 2.1 is true, then 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, we will get the result.

From above discussion 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 2.1 shows. It means that we have a finite sufficient

condition for the constructibility of regular 2^k-sided polygons: 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. By Proposition 2.1 the condition holds for $2\leq k\leq 4$, 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 and F_4 will lead regular 4-sided polygon, regular 8-sided polygon and regular 16-sided polygon to be constructible with compass and straightedge. Hence we have the following generalized condition: A 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 condition is acceptable then every case showed by Gauss-Wantzel theorem will imply existence of direct or indirect connections between Fermat primes and constructible regular polygons.

References

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

[2]. Sierpinski's triangle (Pascal's triangle mod 2) converted to decimal in The On-Line Encyclopedia of Integer Sequences.
http://oeis.org/A001317

[3]. Numbers of edges of regular polygons constructible with ruler and compass in The On-Line Encyclopedia of Integer Sequences.
http://oeis.org/A003401

[4]. 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
http://wenku.baidu.com/view/2c4da6100b4e767f5acfceo2.html

[5]. 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

[6]. 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

[7]. Mersenne prime in The On-Line Wikipedia.
http://en.wikipedia.org/wiki/Mersenne_prime