Why Do All Composite Fermat Numbers Become Pseudoprimes

Pingyuan Zhou

E-mail：zhoupingyuan49@hotmail.com

Abstract

In this paper we present a new and equivalent statement of Fermat's little theorem for Fermat numbers $F_{2^n} \equiv 2 \pmod{F_n}$ by introducing double Fermat number formula $F_{2^n} = 2^{F_n - 1} + 1$, and give a very simple and acceptable explanation for all composite Fermat numbers to be pseudoprimes.

Keywords: Fermat number; composite Fermat number; double Fermat number; Fermat's little theorem; pseudoprime.

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

It is well known that Fermat's little theorem is one of four basic theorems in elementary number theory[1], which is expressed as

$$a^p \equiv a \pmod{p}, \qquad (1)$$

where p is a prime number and a is any integer greater than 1. If a is not divisible by p i.e. a is coprime to p, Fermat's little theorem is equivalent to the statement that $a^{p-1}-1$ is an integer multiple of p:

$$a^{p-1} \equiv 1 \pmod{p}. \qquad (2)$$

For example, if a=2 and p=7, then 2^6=64 and 64–1=63=7×9.

It has been proved that any prime number p satisfies Fermat's little theorem, which includes Fermat primes. But there are some composite numbers also satisfy Fermat's little theorem, in which the smallest such composite number is 341=11×31, so that such composite numbers are called pseudoprimes to base a and 341 is the smallest pseudoprime to base 2[2]. In 1903, Malo showed that if n is a pseudoprime then 2^n-1 is a pseudoprime, hence there are infinitely many pseudoprimes.

If p is a Fermat prime F_n then the Fermat prime must satisfy Fermat's little theorem, and we have

$$2^{F_n-1} \equiv 1 \pmod{F_n}, \qquad (3)$$

because Fermat prime F_n is coprime to base 2. But it has been proved that any composite Fermat number F_n also satisfies the congruences $2^{F_n-1} \equiv 1 \pmod{F_n}$, which means all Fermat numbers satisfy Fermat's little theorem and the congruences $2^{F_n-1} \equiv 1 \pmod{F_n}$ are the statement of Fermat's little theorem for Fermat numbers. From it we see all composite Fermat numbers are pseudoprimes.

Why do all composite Fermat numbers become pseudoprimes? From above statement we see it has been a solved problem. However, when using our definited double Fermat number[3]

$$F_{2^n} = 2^{F_n - 1} + 1, \tag{4}$$

where n is natural number 0, 1, 2, 3, … , we will give a very simple and clear explanation for the problem again.

So-called double Fermat numbers are an infinite subset of Fermat numbers and generated from the recurrence relations $F_{2^{n+1}} = (F_{2^n} - 1)^{F_n - 1} + 1$ with $F_{2^0} = 5$ for $n \geq 0$, and it has been presented that there are only three double Fermat primes i.e. $F_{2^0} = 5$, $F_{2^1} = 17$, $F_{2^2} = 65537$ so that all larger double Fermat numbers than the three numbers are composite[3]. If double Fermat number formula $F_{2^n} = 2^{F_n - 1} + 1$ is introduced, the statement of Fermat's little theorem for Fermat numbers $2^{F_n - 1} \equiv 1 \pmod{F_n}$ can be written the congruences

$$F_{2^n} \equiv 2 \pmod{F_n} \tag{5}$$

to be a new and equivalent statement of Fermat's little theorem for Fermat numbers such as $F_{2^0} \equiv 2 \pmod{F_0}$, $F_{2^1} \equiv 2 \pmod{F_1}$, $F_{2^2} \equiv 2 \pmod{F_2}$, $F_{2^3} \equiv 2 \pmod{F_3}$, $F_{2^4} \equiv 2 \pmod{F_4}$ and $F_{2^5} \equiv 2 \pmod{F_5}$[4]. Considering the property involving Fermat numbers that $F_n - 2$ is divisible by all smaller Fermat numbers i.e. $F_n = F_0 F_1 F_2 \ldots F_{n-1} + 2$[5], we discover the congruences $F_{2^n} \equiv 2 \pmod{F_n}$ just present this well-known property, because we will have $F_m = F_0 F_1 F_2 \ldots F_{m-1} + 2$ if let $m = 2^n$ here. It implies that the congruences $F_{2^n} \equiv 2 \pmod{F_n}$ are a special case of the property involving Fermat numbers for $m = 2^n$, so that formula (5) can be written

$$F_m \equiv 2 \pmod{F_n}, \tag{6}$$

where $m = 2^n$. Formula (6) is just the equivalent statement of Fermat's little theorem for Fermat numbers. In other words, Because of existence of the property involving Fermat numbers that F_n–2 is divisible by all smaller Fermat numbers, the equivalent statement of Fermat's little theorem for Fermat numbers $F_{2^n} \equiv 2$ (mod F_n) can be written formula (6) to be just a special expression of the property involving Fermat numbers, which clearly implies all composite Fermat numbers to be pseudoprimes.

References

[1]. Fermat's little theorem in The On-Line Wikipedia.
http://en.wikipedia.org/wiki/Fermat%27s_Little_Theoram

[2]. Pseudoprime in The On-Line Wikipedia.
http://en.wikipedia.org/wiki/Pseudoprime

[3]. Pingyuan Zhou, On the Connections between Mersenne and Fermat Primes, Global Journal of Pure and Applied Mathematics 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

[4]. Pingyuan Zhou, Catalan-type Fermat Numbers, Global Journal of Pure and Applied Mathematics 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

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