PLACED NEAR THE FERMAT PRIMES AND THE FERMAT COMPOSITE NUMBERS

Ikorong Anouk Gilbert Nemron
Centre De Calcul, D'Enseignement Et De Recherche,
Universite' de ParisVI, France
Email: ikorong@ccr.jussieu.fr

ABSTRACT

In this paper, we show a Theorem which helps to characterize the Fermat primes and the Fermat composite numbers. We recall that a *Fermat prime* (see [1] or [2] or [3]) is a prime of the form $F_m = 2^{2^m} + 1$, where m is an integer ≥ 0; for example F_0 and F_1 and F_2 and F_3 and F_4 are *Fermat prime*. A *Fermat composite number* or a *Fermat composite* (see [1] or [2] or [3]) is a non prime number of the form $F_m = 2^{2^m} + 1$, where m is an integer ≥ 1. it is known that F_5 and F_6 are Fermat composite; and Fermat composite are known for some integers $> F_6$.

AMS Classification 2000: 05xx and 11xx.
Key words: *Fermat primes and Fermat composite.*

INTRODUCTION

This paper is divided into two sections. In section.**1**, we state and prove a Theorem which implies the characterizations of the Fermat primes and the Fermat composite numbers. In section.**2**, using the Theorem of section.**1**, we characterize the Fermat primes and the Fermat composite numbers.

1. STATEMENT AND THE PROOF OF THEOREM WHICH IMPLIES THE CHARACTERIZATIONS OF THE FERMAT PRIMES AND THE FERMAT COMPOSITE NUMBERS

We recall that for every integer $n \geq 1$, $n!$ is defined as follow:

$$n! = \begin{cases} 1 & \text{if } n = 1, \\ 2 & \text{if } n = 2, \\ 1 \times 2 \times .... \times n & \text{if } n \geq 3. \end{cases}$$

THEOREM 1.1. *Let* m *be an integer* ≥ 1*, and look at* 2^{2^m}*. Then,* $2^{2^m} + 1$ *is prime or* $2^{2^m} + 1$ *divides* $(2^{2^m})!$.

Before simply proving Theorem 1.1, let us remark the following.

REMARK 1.2. *Let* m *be an integer* ≥ 1*; and put* $n = 2^{2^m}$*. If* $n + 1 = p^2$ *(where* p *is prime), then* $n + 1$ *divides* $n!$.

Proof. Otherwise [we reason by reduction to absurd], clearly

$$p^2 \text{ does not divide } n! \qquad \textbf{(1.2.0)},$$

and we observe the following.

Observation 1.2.1. p *is a prime* ≥ 3.

Otherwise, clearly $p = 2$, and noticing (via the hypotheses) that $n + 1 = p^2$, then using the previous two equalities, it becomes trivial to deduce that $n = 3$; a contradictionn, since $n \geq 4$ (via the hypotheses).

Observation $1.2.2.$ $p \le n$.
Otherwise, $p > n$ and the previous inequality clearly says that

$$p \ge n+1 \tag{1.2.2.0}$$

Now noticing (via the hypotheses) that $n+1 = p^2$, then, using the previous equality and using *(1.2.2.0)*, we trivially deduce that

$$p \ge n+1 and\, n+1 = p^2 \tag{1.2.2.1}$$

(1.2.2.1) clearly says that $p \ge p^2$; a contradiction, since $p \ge 3$ (by using Observation $1.2.1$).
Observation $1.2.3.$ $2p \le n$.
Otherwise, $2p > n$ and the previous inequality clearly says that

$$2p \ge n+1 \tag{1.2.3.0}$$

Now noticing (via the hypotheses) that $n+1 = p^2$, then, using the previous equality and using *(1.2.3.0)*, we trivially deduce that

$$2p \ge n+1 and\, n+1 = p^2 \tag{1.2.3.1}$$

(1.2.3.1) clearly says that $2p \ge p^2$; a contradiction, since $p \ge 3$ (by using Observation $1.2.1$). Observation $1.2.3$ follows.
Observation $1.2.4.$ $2p \ne p$.
Indeed, it is immediate that $2p \ne p$, since $p \ge 3$ (by using Observation $1.2.1$). Observation $1.2.4$ follows.
The previous trivial observations made, look at p (recall that p is prime); observing (by Observations $1.2.2$ and $1.2.3$ and $1.2.4$) that $p \le n$ and $2p \le n$ and $p \ne 2p$, then, it becomes trivial to deduce that

$$\{p, 2p\} \subseteq \{1,2,3,.....,n-1,n\} \tag{1.2.5}$$

(1.2.5) immediately implies that

$$p \times 2p \; divides \; 1 \times 2 \times 3 \times ... \times n-1 \times n \tag{1.2.6}$$

(1.2.6) clearly says that $2p^2$ divides $n!$; in particular p^2 clearly divides $n!$ and this contradicts **(1.2.0)**. Remark 1.2 follows.
The previous remark made, now we prove simply Theorem $1.1.$

Proof of Theorem $1.1.$ Put $n = 2^{2^m}$ and look at $n+1$. **If** $n+1$ is prime, then the proof is ended. **If** $n+1$ is not prime, then $n+1$ divides $n!$. Otherwise (we reason by reduction absurd)

$$n+1 \text{ is not prime and } n+1 \text{ does not divide } n! \tag{1.1.0}$$

and we observe the following.

Observation $1.1.1.$ *Let* p *be a prime such that* $n+1$ *is divisible by* p *(such a* p *clearly exists). Then* $\frac{n+1}{p}$ *is an integer* **and** $\frac{n+1}{p} \le n$ **and** $p \le n$ **and** $\frac{n+1}{p} = p$.

Indeed, it is immediate that $\frac{n+1}{p}$ is an integer [since p divides $n+1$], **and** it is also immediate that $\frac{n+1}{p} \le n$ [otherwise, $n+1 > np$; now, remarking that $p \ge 2$ (since p is prime), then the previous two inequalities imply

that $n+1>2n$; so $1>n$ and we have a contradiction, since $n\geq 4$, by the hypotheses]. **Clearly** $p\leq n$ [otherwise, $p>n$; now, recalling that $n+1$ is divisible by p, then the previous inequality implies that $n+1=p$. Recalling that p is prime, then the previous equality clearly says that $n+1$ is prime and this contradicts **(1.1.0)**]. That being so, to prove Observation $1.1.1$, it suffices to prove that $\frac{n+1}{p}=p$. **Fact:** $\frac{n+1}{p}=p$ [otherwise, clearly $\frac{n+1}{p}\neq p$; now, remarking (by using the previous) that $\frac{n+1}{p}$ is an integer **and** $\frac{n+1}{p}\leq n$ **and** $p\leq n$; then it becomes trivial to deduce that $\frac{n+1}{p}$ **and** p are two different integers such that $\{p,\frac{n+1}{p}\}\subseteq\{1,2,3,.....,n-1,n\}$. The previous inclusion immediately implies that $p\times\frac{n+1}{p}$ divides $1\times 2\times 3\times ...\times n-1\times n$; therefore $n+1$ divides $n!$, and this contradicts **(1.1.0)**. So $\frac{n+1}{p}=p$]. Observation $1.1.1$ follows.

The previous trivial observation made, look at $n+1$; observing (by using Observation $1.1.1$) that p is prime such that $\frac{n+1}{p}=p$, clearly

$$n+1=p^2, where\ p\ is\ prime \tag{1.1.2}$$

Now using *(1.1.2)* and Remark 1.2, then it becomes trivial to deduce that $n+1$ divides $n!$, and this contradicts **(1.1.0)**. Theorem 1.1 follows.

Theorem 1.1 immediately implies the characterizations of Fermat primes and Fermat composite numbers.

2. CHARACTERIZATIONS OF FERMAT PRIMES AND FERMAT COMPOSITE NUMBERS

In this section, using Theorem 1.1, we characterize Fermat primes and Fermat composite numbers.

THEOREM 2.1. *(Characterization of Fermat primes). Let* m *be an integer* ≥ 1 *and look at* $2^{2^m}+1$. *Then the following are equivalent.*

(1). $2^{2^m}+1$ is a Fermat prime.

(2). $2^{2^m}+1$ does not divide $(2^{2^m})!$.

To prove simply Theorem 2.1, we need a Theorem of Euclide.

THEOREM 2.2 *(Euclide). Let* a, b *and* c, *be integers such that* $a\geq 1$, $b\geq 1$ *and* $c\geq 1$. *If* a *divides* bc *and if the greatest common divisor of* a *and* b *is* 1, *then* a *divides* c.

COROLLARY 2.3. *Let* n *be an integer* ≥ 1 *and look at* $n!$. *Now let* p *be a prime* $\geq n+1$*; then the greatest common divisor of* $n!$ *and* p *is* 1 *(in particular,* p *does not divide* $n!$*).*

Proof. Immediate, and follows immediately by using Theorem 2.2 and the definition of $n!$, and by observing that p is a prime $\geq n+1$.

Now, we simply prove Theorem 2.1.

Proof of Theorem 2.1. $(1)\Rightarrow(2)$]. Immediate, by puting $n=2^{2^m}$ and by remarking that $n+1$ is prime and by using Corollary 2.3.

$(2) \Rightarrow (1)$]. Immediate. Indeed, since $2^{2^m}+1$ does not divide $(2^{2^m})!$, then, using Theorem 1.1, we immediately deduce that $2^{2^m}+1$ is prime, and therefore, $2^{2^m}+1$ is a Fermat prime.
Using Theorem 2.1, then the following Theorem becomes immediate.

THEOREM 2.4. *(Characterization of Fermat composite numbers). Let* m *be an integer* ≥ 1 *and look at* $2^{2^m}+1$. *Then the following are equivalent.*

(1). $2^{2^m}+1$ is a Fermat composite number.

(2). $2^{2^m}+1$ divides $(2^{2^m})!$.

Proof. Immediate and follows by using Theorem 2.1.

REFERENCES

[1]. Ikorong Anouk Gilbert Nemron. *An original symposium over the Goldbach conjecture, The Fermat primes, The Fermat composite numbers conjecture, and the Mersenne primes conjecture* .Mathematicae Notae. Vol XLV(2008). 31-39.

[2]. Ikorong Anouk Gilbert Nemron. *A Glance At A Different Kinds Of Numbers.* International Journal Of Mathematics And Computer Sciences. Vol.4, No.1, 2009. 43-53.

[3]. Iorong Anouk Gilbert Nemron. *Runing With The Twin Primes, The Goldbach Conjecture, The Fermat Primes Numbers, The Fermat Composite Numbers, And The Mersenne Primes*; Far East Journal Of Mathematical Sciences; Volume 40, Issue 2, May 2010, 253-266.