Journal of Progressive Research in Mathematics(JPRM)
ISSN: 2395-0218

SCITECH
RESEARCH ORGANISATION|

Volume 16, Issue 4

Published online: September 22, 2020|

Journal of Progressive Research in Mathematics
www.scitecresearch.com/journals

An Original note on Fermat numbers, on numbers of the form W_n and on numbers of the form $10k + 8 + Fn$ [where $W_n \in \{22 + F_n, 2^n + F_n\}$, n is an integer ≥ 0, F_n is a Fermat number and k is an integer ≥ 0]

Ikorong Annouk,

Centre De Calcul; D'Enseignement Et De Recherche En
Mathematiques Pures. ikorong@ccr.jussieu.fr
Paul Archambault. Paul.Archambault@precisely.com

Abstract and Definitions. A *Fermat number* is a number of the form $F_n = 2^{2^n} + 1$, where n is an integer ≥ 0. A *Fermat composite* (see [1] or [2] or [4]) is a non prime *Fermat number*. Fermat composites and Fermat primes are characterized via divisibility in [4] and [5] (A *Fermat prime* (see [1] or [2] or [4]) is a prime *Fermat number*). It is known (see [4]) that for every $j \in \{0, 1, 2, 3, 4\}$, F_j is a Fermat prime and it is also known (see [2] or [3]) that F_5 and F_6 are Fermat composites. In this paper, we show [via elementary arithmetic congruences] the following result (**T.**). *For every integer* $n \geq 2$, $F_n - 1 \equiv 1\, mod[j]$ *(where* $j \in \{3, 5\}$*).* Result (**T**) immediately implies that *for every fixed integer* $k \geq 0$*, there exists at most two primes of the form* $10k + 8 + F_n$ [in particular , for every fixed integer $k \geq 0$, the numbers of the form $10k + 8 + F_n$ (where n is an integer ≥ 2) are all composites]. Result (**T.**) also implies that there are infinitely many composite numbers of the form $2^n + F_n$ and there exists no prime number of form $22 + F_n$. Result (**T.**) coupled with a special case of a Theorem of Dirichlet on arithmetic progressions help us to explain why it is natural to conjecture that there are infinitely many Fermat primes.

Keywords: Fermat number, F_n.
AMS Classification 2000: 05xx and 11xx

Theorem 1.1.
(**T.**). *For every* $n \geq 2$, $F_n - 1 \equiv 1\, mod[j]$ *(where* $j \in \{3, 5\}$*).*
(**T.1**). *For every fixed integer* $k \geq 0$*, there exists at most two primes of the form* $10k + 8 + F_n$.
(**T.2**). *For every fixed integer* $k \geq 0$*, the numbers of the form* $10k + 8 + F_n$ *[where* n *is an integer* ≥ 2 *] are all composites.*
(**T.3**). *There are infinitely many composite numbers of the form* $2^n + F_n$.
(**T.4**). *There exists no prime number of the form* $22 + F_n$.

To prove Theorem 1.1, we need the following remarks.

Remark 1.0. *Let n be an integer ≥ 3. If $2^{2^{n-1}} \equiv 1\, mod[j]$ where $j \in \{3,5\}$, then $2^{2^{n-1}} \times 2^{2^{n-1}} \equiv 1\, mod[j]$.* (*Proof.* Immediate [via elementary arithmetic congruences]. □)

Proposition 1.1. *Let n be an integer ≥ 2, then $2^{2^n} \equiv 1\, mod[j]; j \in \{3,5\}$.*
(*Proof.* Otherwise

$$let\, n\, be\, minimum\, such\, that\, 2^{2^n} \not\equiv 1\, mod[j]; \;\; j \in \{3,5\} \qquad (1.1).$$

Clearly

$$n \geq 3 \qquad (1.2)$$

(since $2^{2^2} = 16$ and $16 \equiv 1\, mod[j]$ where $j \in \{3,5\}$). It is immediate to see that

$$2^{2^n} = 2^{2^{n-1}} \times 2^{2^{n-1}} \qquad (1.3).$$

Now using equality *(1.3)* and inequality *(1.2)*, we easily deduce that *(1.1)* clearly implies that

$$2^{2^{n-1}} \times 2^{2^{n-1}} \not\equiv 1\, mod[j],\; where\, j \in \{3,5\}\, and\, where\;\; 2^{2^{n-1}} \equiv 1\, mod[j];\; (n \geq 3) \qquad (1.4).$$

(1.4) clearly contradicts Remark 1.0. □)

Remark 1.2. *Let n be an integer ≥ 3. If $2 \times 2^{n-1} \equiv 0\, mod[3]$, then $2^{n-1} \equiv 0\, mod[3]$.* (*Proof.* Immediate [via elementary arithmetic congruences and the fact that $2 \equiv 2 mod[3]$]. □)

Proposition 1.3. *Let n be an integer ≥ 2; then $2^n \not\equiv 0\, mod[3]$.*
(*Proof.* Otherwise

$$let\, n\, be\, minimum\, such\, that\, 2^n \equiv 0\, mod[3] \qquad (1.5).$$

Clearly

$$n \geq 3 \qquad (1.6)$$

(since $2^2 = 4$ and $4 \not\equiv 0\, mod[3]$). It is immediate to see that

$$2 \times 2^{n-1} = 2^n \qquad (1.7).$$

Now using equality *(1.7)* and inequality *(1.6)*, we easily deduce that *(1.5)* clearly implies that

$$2 \times 2^{n-1} \equiv 0\, mod[3],\; where\, 2^{n-1} \not\equiv 0\, mod[3];\; n \geq 3 \qquad (1.8).$$

(1.8) clearly contradicts Remark 1.2. □)

Proposition 1.4. *Let n be an integer ≥ 2 and let k be a fixed integer ≥ 0 [k is fixed once and for all, so k does not move anymore]. Then $10k + 8 + F_n \equiv 0\, mod[5]$ and $10k + 8 + F_n$ is composite.*
(*Proof* (i). *$8 + F_n \equiv 0\, mod[5]$ and $8 + F_n$ is composite.* Clearly

$$(2^{2^n} + 1) + 8 \equiv 0\, mod[5] \qquad (1.9)$$

[use Proposition 1.1 and elementary arithmetic congruences]. So $8 + F_n \equiv 0\, mod[5]$ and $8 + F_n$ is composite [use congruence *(1.9)* and observe that $(2^{2^n} + 1) + 8 = 8 + F_n$ and $8 + F_n > 5$ (note that $n \geq 2$)].
(ii). $10k + 8 + F_n \equiv 0\, mod[5]$ *and* $10k + 8 + F_n$ *is composite.* Immediate (use (i) and observe that $10k \equiv 0\, mod[5]$). Proposition 1.4 immediately follows [use (i) and (ii)]$\Big)$.□

Proposition 1.5. *Let n be an integer ≥ 2. Then $22 + F_n \equiv 0\, mod[3]$ and $22 + F_n$ is composite.*
$\Big($ *Proof.* Clearly

$$22 + (2^{2^n} + 1) \equiv 0\, mod[3] \tag{1.10}$$

[observe that $2^{2^n} \equiv 1\, mod[3]$ (use Proposition 1.1) and use elementary arithmetic congruences]. So $22 + F_n \equiv 0\, mod[3]$ and $22 + F_n$ is composite [use congruence *(1.10)* and observe that $22 + (2^{2^n} + 1) = 22 + F_n$ and $22 + F_n > 3$ (note that $n \geq 2$)]. Proposition 1.5 immediately follows$\Big)$.□

Proposition 1.6. *Let n be an integer ≥ 3 and let $B_n = 2^n + F_n$; then there exists $j \in \{0, 1\}$ such that B_{n+j} is composite.*
$\Big($ *Proof.* (i'). *If $2^n \equiv 2\, mod[3]$, then the number B_{n+j} is composite, where $j = 1$.* Indeed if $2^n \equiv 2\, mod[3]$, clearly

$$2 \times 2^n \equiv 1\, mod[3] \tag{1.11}$$

[use elementary arithmetic congruences] and so

$$2^{n+1} \equiv 1\, mod[3] \tag{1.12}$$

[use *(1.11)* and observe that $2 \times 2^n = 2^{n+1}$]. Observe (via Proposition 1.1) that

$$2^{2^{n+1}} \equiv 1\, mod[3] \quad (1.13),$$

and so

$$2^{2^{n+1}} + 1 \equiv 2\, mod[3] \tag{1.14}$$

[use *(1.13)* and elementary arithmetic congruences]. Clearly

$$2^{n+1} + (2^{2^{n+1}} + 1) \equiv 0 \mod [3] \tag{1.15}$$

[use *(1.12)* and *(1.14)* and elementay arithmetic congruences]. Clearly

$$2^{n+j} + F_{n+j} \equiv 0\, mod[3]\, where\, j = 1 \tag{1.16}$$

[use *(1.15)* and observe that $2^{n+1} + (2^{2^{n+1}} + 1) = 2^{n+j} + F_{n+j}$, where $j = 1$] and so B_{n+j} is composite, where $j = 1$ [use *(1.16)* and observe that $B_{n+1} = 2^{n+1} + F_{n+1}$ and $B_{n+1} > 3$ since $n \geq 3$].
(ii'). *If $2^n \not\equiv 2\, mod[3]$, then the number B_{n+j} is composite, where $j = 0$.* Indeed if $2^n \not\equiv 2\, mod[3]$, then

$$2^n \equiv 1\, mod[3] \tag{1.17}$$

[use Proposition 1.3, by observing that $2^n \equiv k\, mod[3]$ if and only if $k \in \{0, 1, 2\}$]. Now observe (by Proposition 1.1) that

$$2^{2^n} \equiv 1\, mod[3] \quad (1.18),$$

and so

$$2^{2^n} + 1 \equiv 2\, mod[3] \tag{1.19}$$

[use *(1.18)* and elementary arithmetic congruences]. Clearly

$$2^n + (2^{2^n} + 1) \equiv 0 \mod [3] \qquad (1.20)$$

[use *(1.17)* and *(1.19)* and elementay arithmetic congruences]. Clearly

$$2^{n+j} + F_{n+j} \equiv 0\, mod[3]\, where\, j = 0 \qquad (1.21)$$

[use *(1.20)* and observe that $2^n + (2^{2^n} + 1) = 2^{n+j} + F_{n+j}$, where $j = 0$] and so B_{n+j} is composite, where $j = 0$ [use *(1.21)* and observe that $B_n = 2^n + F_n$ and $B_n > 3$ since $n \geq 3$]. Proposition 1.6 immediately follows [use (**i'**) and (**ii'**)]).□

Remark 1.7. *There are infinitely many composite numbers of the form $2^n + F_n$ or there are infinitely many prime numbers of the form $2^n + F_n$.*
(*Proof.* Immediate). □

Having made the previous Remarks and Propositions, then Theorem 1.1 becomes immediate to prove.

Proof of Theorem 1.1.
(**T.**). Immediate [use Proposition 1.1, and observe that $2^{2^n} = F_n - 1$].
(**T.1**). Immediate [observe that $10k + 8 + F_0 = 10k + 11$ and $10k + 8 + F_1 = 10k + 13$; and use Proposition 1.4].
(**T.2**). Immediate [use Proposition 1.4].
(**T.3**). Immediate [use Proposition 1.6 and Remark 1.7].
(**T.4**). Immediate [observe that $22 + F_0 = 25$ and $22 + F_1 = 27$; and use Proposition 1.5].□

Now using Result (**T.**), then we end this note by looking at Fermat primes.

Observation. *It is natural to conjecture that there are infinitely many Fermat primes.*

Indeed observing [via Result (**T.**) of Theorem 1.1] that

$$F_n - 1 \equiv 1\, mod[3]\, and\, F_n - 1 \equiv 1\, mod[5]\;\; for\, every\, integer\, n \geq 2 \qquad (1.22),$$

clearly

$$F_n \equiv 2\, mod[5]\, and\, F_n \equiv 2\, mod[3]\;\; for\, every\, integer\, n \geq 2 \qquad (1.23),$$

[use *(1.22)* and elementary arithmetic congruences].
Now let $A_{2.5} = \{e;\, e\, is\, prime\, and\, e \equiv 2\, mod\,[5]\}$ and let $A_{2.3} = \{e';\, e'\, is\, prime\, and\, e' \equiv 2\, mod\,[3]\}$.
Since it is immediate that

$$(2,5) = 1\, and\, (2,3) = 1\, [i.e.\, (2,5)\, and\, (2,3)\, are\, two\, couple\, of\, positive\, coprime\, integers] \quad (1.24),$$

then using *(1.24)* coupled with a special case of a Theorem of Dirichlet on arithmetic progressions, it follows that

$$card(A_{2.5})\, is\, infinite\, and\, card(A_{2.3})\, is\, infinite \qquad (1.25).$$

Now using *(1.23)* and *(1.25)* and the fact that for every $n \in \{0, 1, 2, 3, 4\}$ F_n is prime and $F_n \in A_{2.5} \bigcup A_{2.3}$ [use Abstract and definitions for F_n and *(1.23)* and the definition of $(A_{2.5}, A_{2.3})$] , then it becomes naturel to conjecture the following.

Conjecture. *$A_{2.5} \bigcup A_{2.3}$ contains infinitely many F_n ($A_{2.5}$ and $A_{2.3}$ are defined via the Observation placed just above).*

Observing that $A_{2.5}$ and $A_{2.3}$ are two infinite set of prime numbers, then the previous conjecture immediately implies that there are infinitely many Fermat primes.

References

[1] Dickson. *Theory of Numbers (History of Numbers. Divisibity and primality) Vol* 1. *Chelsea Publishing Company*. *New York*, *N.Y (*1952*)*. Preface.*III* to Preface.*XII*.

[2] G.H Hardy, E.M Wright. *An introduction to the theory of numbers. Fith Edition. Clarendon Press. Oxford*.

[3] Paul Hoffman. *Erdös*, *l'homme qui n'aimait que les nombres*. *Editions Belin*, (2000). 30-49.

[4] Ikorong Annouk. *Placed Near The Fermat Primes And The Fermat Composite Numbers*. International Journal Of Research In Mathematic And Apply Mathematical Sciences; Vol3; 2012, 72 - 82.

[5] Ikorong Annouk. *Then We Characterize Primes and Composite Numbers Via Divisibility*. International Journal of Advanced In Pure Mathematical Sciences; Volume 2, no.1; 2014.