NNTDM 11 (2005) 4, 17-24

FERMAT AND MERSENNE NUMBERS

J. V. Leyendekkers
The University of Sydney, 2006, Australia

A. G. Shannon
Warrane College, The University of New South Wales, Kensington, 1465, &
KvB Institute of Technology, North Sydney, NSW 2060, Australia

Abstract

Fermat numbers $\left(F_n = 2^{2^n} + 1\right)$ and Mersenne numbers $\left(M_m = 2^m - 1\right)$ m odd are compared on the basis of integer structure, using the modular rings Z_4 and Z_6. The two numbers fall in different classes and this results in different composite row structures and different potentials for the formation of primes. The constraints on 2^n and the right end digits for F_n result in fewer numbers over a given range than those for M_m. This is shown with two functions which link the two numbers and show that $F_n = \left(2^{x^2+y^2-1} + 1\right)$: for primes $y = n$, but when n>4, $y \neq n$.

1. Introduction

The Fermat numbers $\left(F_n = 2^{2^n} + 1\right)$ and Mersenne numbers $\left(M_m = 2^m - 1\right)$ m odd have been known for centuries with interest centred on which n,m yield primes. We show here that when investigated on the basis of integer structure, further interesting properties of these numbers can be revealed. Modular rings, Z_i, provide useful frameworks for integer structure: here we utilise Z_4 and Z_6 [6,7,10]. The integers in these rings have the forms $4r_i + i$, and $6r_i + (i-3)$, where $\bar{i}$ is the class and r the row in a tabulated array (Table 1).

Modular Ring	'Even' Classes	'Odd' Classes	Comments
Z_4	$\bar{0}_4,\ \bar{2}_4$	$\bar{1}_4,\ \bar{3}_4$	$\bar{2}_4$ has no powers; $\bar{3}_4$ has no even powers
Z_6	$\bar{1}_6, \bar{3}_6, \bar{5}_6$	$\bar{2}_6, \bar{4}_6, \bar{6}_6$	$3\|M,\ M \in \{\bar{3}_6, \bar{6}_6\}$; no even powers $\in \{\bar{5}_6, \bar{2}_6\}$

Table 1: Classification of the Classes of the two Rings

Distinct Fermat numbers are relatively prime [5], and all numbers of the form $2^n m$, where the distinct prime factors of m are Fermat primes or primes in the Class Z_3, with at most eight of the latter [3]. Moreover, F_n seems to yield fewer primes than M_m in any given range. This motivates us to compare their characteristics by means of the 'row structures' within these rings and to express each type of number as a function of the other.

2. Comparisons of Fermat and Mersenne Numbers

A variety of pertinent properties of the two numbers is listed in Table 2.

Classes and rows. In Z_6, since $\bar{2}_6$ has no even powers, there is more room for primes than in $\bar{4}_6$ and these primes are distributed more or less equally between odd and even rows. However, in $\bar{4}_6$ primes are more dominant in odd rows. This is understandable since the squares are in the even rows and there is less room there for primes. Since Mersenne numbers fall in $\bar{4}_6$ in odd rows this is compatible with their falling in Class $\bar{3}_4 \in Z_4$. $\bar{3}_4$ has more room for primes than $\bar{1}_4$ ($\bar{3}_4$ having no even powers). On the other hand, the fact that F_n rows are odd carries no prime bias because of the equivalence of even and odd rows in $\bar{2}_6$. Furthermore, being in $\bar{1}_4 \subset Z_4$ means less abundance of primes.

Property	$F_n = 2^{2^n}+1$	$M_m = 2^m - 1$
Class	$\bar{2}_6 \in Z_6,\ \bar{1}_4 \in Z_4$	$\bar{4}_6 \in Z_6,\ \bar{3}_4 \in Z_4$
Parity of rows	Z_6 *odd* (R_2), Z_4 *odd / even* (r_4)	Z_6 *odd* (R_4), Z_4 *odd / even* (r_3)
Rows for composites in Z_6	$R_2 = \frac{1}{3}\left(\frac{1}{2}\left(p^2+1\right)+ap\right)+pt$, $a=1,\ p\in\bar{2}_6;\ a=2,\ p\in\bar{4}_6$, t=0,1,2,3,…; p lowest prime factor	$R_4 = \frac{1}{6}\left(p^2-1\right)+pt,\ t$ odd
Rows in Z_6 which correspond to those in $\bar{3}_4 \in Z_4$	R_2 *even* $\left(\bar{2}_6\right)$	R_4 *odd* $\left(\bar{4}_6\right)$
Class 2^m	$Z_6\ \ \bar{1}_6$ *odd & even* $Z_4\ \ \bar{0}_4$ *powers*	$Z_6\ \ \bar{5}_6$ (*no even powers*) $Z_4\ \ \bar{0}_4$ (*odd & even powers*)
$M = x^2 + y^2$	$F_n = M$	$M_m \neq M$
Factors	$\left(2^{\frac{m}{2}}-i\right)\left(2^{\frac{m}{2}}+i\right)$ *equal* $\left(x^2+y^2\right)$ [*see Section* 6]	$\left(2^{\frac{m}{2}}-1\right)\left(2^{\frac{m}{2}}+1\right)$ *can equal* $\left(x^2+y^2\right)$ *but not commonly*
Right end digits (REDs) M>5	7	1 and 7
Tests for primes	Pépin [12]	Lucas [12]
m values for primes	n 0,1,2,3,4; m 1,2,4,8,16.	3,5,7,13,17,19,31,61,89,107,127,…[8]
Number of primes for $m \le 139267$	5	33

Table 2: Properties of Fermat & Mersenne Numbers

Right end digits (REDs). For Fermat numbers the RED is confined to 7, whereas Mersenne numbers have twiqce the opportunity of occurring since the REDs equal 1 or 7.

Character of *m*. Fermat numbers are restricted to $m = 2^n$ so that $m_i = 2m_{i-1}$. On the other hand, Mersenne numbers have unrestricted odd numbers for *m*. Although a prime Mersenne number only occurs when *m* is a prime. Nevertheless, for a given range $M_m \geq F_n$ (Table 2).

Composites. There are more composite rows available for F_n since *t* can be odd or even (Table 2), whereas for M_m *t* must be odd to conform to the parity of the row (odd). Thus there is more opportunity for composite formation with F_n.

3. Row Structure of M_m

The row structure of composite Fermat numbers has been discussed previously [11]. When Mersenne numbers, M_m, are composite, even when *m* is prime, they fall in rows given by [10]:

$$R_4 = R' + pt \tag{3.1}$$

where

$$R' = \tfrac{1}{6}\left(p^2 - 1\right), M_m \in \overline{4}_6,$$

so that

$$\begin{aligned} M_m &= 6R_4 + 1 \\ &= p^2 + 6pt, \end{aligned} \tag{3.2}$$

so that, in turn,

$$t = \tfrac{1}{6p}\left(M_m - p^2\right) \tag{3.3}$$

but

$$M_m = pN$$

where *p* is the lowest prime factor, so that

$$t = \tfrac{1}{6}\left(N - p\right). \tag{3.4}$$

t may be estimated because factors of Mersenne numbers are known for a large number of *m* values [2,12].

It is found that *m* is always a factor of *t* (Table 3). With *t*=*mx*, *x* has certain interesting characteristics (Table 3). When *m* produces a prime $\left(m = p_i\right)$, the previous prime value of *m* $\left(m = p_{i-1}\right)$has *x* values that are primes, while $m = p_{i-2}$ has 3|*x*. (For recent research on consecutive prime numbers, see [1].)

4. Mersenne Numbers and Fermat Numbers as Functions of One Another

Mersenne numbers may be expressed as functions of Fermat numbers as follows. Since [11]

$$\begin{aligned} \mathrm{F_n} &= \left(\prod_{j=0}^{n-1} F_j + 2 \right) \\ &= 2^m + 1,\ m = 2^n, \end{aligned} \tag{4.1}$$

$$\begin{aligned} M_{m+q} &= \left(2^{m+q} - 1\right) \\ &= 2^q \left(\prod_{j=0}^{n-1} F_j + 1 \right) - 1 \end{aligned} \tag{4.2}$$

where q is odd (Table 4). Of course,

$$\prod_{J=0}^{N-1} F_J = \left(F_{n-1} - 2\right) F_{n-1}$$

which may be substituted in Equation (4.2).

m	Class	t	Factors of t	M_m
11	$\overline{2}_6$	11	11x1	23 x 89
23	$\overline{2}_6$	29739	23 x3 x431	47 x 178481
29	$\overline{2}_6$	383989	29 x 13241	233 x 1103 x 2089
37	$\overline{4}_6$	102719659	37 x 7 x 3966601	223 x 616318177
41	$\overline{2}_6$	27416331	41 x 3^2 x 191 x 389	13367 x 164511353
43	$\overline{4}_6$	3401428011	43 x 3 x 53 x 499 x 997	431 x 9719 x 2099863
47	$\overline{2}_6$	9977136171	47 x 3 x 17 x 4162343	2351 x 4513 x 13264529
53	$\overline{2}_6$	236000608245	53 x 3 x 5 x 296856111	6361 x 69431 x 20394401
59	$\overline{2}_6$	533905266731	59 x 9049241809	179951 x 3203431780337
67	$\overline{4}_6$	126940758261	67 x 3 x 631546061	193707721 x 761838257287

Table 3: Composites of M_m

m	q	n	$\prod_{j=0}^{n-1} F_j + 1$	M_{m+q}
4	1	2	3 x 5+1	31
8	–1	3	3 x 5 x 17+1	127
8	3	3	3 x 5 x 17+1	2047
16	1	4	3 x 5 x 17 x 257+1	131071

Table 4: Fermat and Mersenne Numbers

Alternatively, for Fermat numbers as function of Mersenne numbers, we have

$$F_{n-1} = \tfrac{1}{2}\left(2 + \left(2M_{m+1} + 2\right)^{\frac{1}{2}}\right),\ m = 2^n. \tag{4.3}$$

Furthermore, since

$$2\left(2^m+1\right)-3=2^{m+1}-1,$$

we have

$$F_n=\tfrac{1}{2}\left(3+M_{m+1}\right). \tag{4.4}$$

For example,

$$F_4=\tfrac{1}{2}\left(3+M_{17}\right)=\tfrac{1}{2}\left(3+131071\right)=65537.$$

Now, $(m+1)=2,3,5,9,17,33,\ldots$; $(m+1)\in\bar{1}_4$, for $(m+1)>3$, and so

$$m+1=x^2+y^2 \tag{4.5}$$

and

$$F_n=2^{x^2+y^2-1}+1. \tag{4.6}$$

n	2	3	4	5	6	7	8	9	10	11	12	13
m	4	8	16	32	64	128	256	512	1024	2048	4096	8192
x	1	0	1	-	1	-	1	-	1	-	1	-
y	2	3	4	-	8	-	16	-	32	-	64	-

Table 5: Characteristics of Fermat numbers as primes

As can be seen from Table 5, the characteristics of F_n as a prime is that $y=n$, and when $x=1$, $n^2=2^n$ and when $x=0$, $n^2-1=2^n$. These characteristics cannot be achieved for $n>4$ as y increases progressively, or no sum of squares exists. The reason some members of Class $\bar{1}_4\subset Z_4$ are not sums of squares has been discussed previously [8]. All such integers are composites. Table 5 also shows that when $m=2^n+1, M_m$ is not a prime when $n>4$. For the range here, $m=257$ is the only prime when $n>4$ and $2^{257}-1$ has three factors.

We have previously shown [9] that

$$N^2=3N+q-2 \tag{4.7}$$

where

$$q=2\sum_{t=0}^{N-2}t=(N-1)(N-2)$$

with N any integer. Thus

$$q_{n-1}=F_n-F_{n-1}=2^{2m}-2^m$$

with $m=2^n$, and since $2^m, 2^{2m}\in\bar{1}_6, q_{n-1}\in\bar{3}_6$, so that $3\,|\,q_{n-1}$.

As well,

$$F_n-F_{n-1}=\sum_{j=2^{n-1}}^{2^n-1}2^j. \tag{4.8}$$

Then since

$$2^{2^n-1}-1=1+\sum_{j=1}^{2^n-2}2^j \tag{4.9}$$
$$=1+\sum_{j=1}^{2^{n-1}-2}2^j+\tfrac{1}{2}\left(F_n-F_{n-1}\right).$$

For example, when n=4,

$$M_{15}=2^{15}-1=32767,$$

and

$$1+\sum_{j=1}^{6}2^j+\tfrac{1}{2}\left(F_4-F_3\right)=32767.$$

5. Mersenne and Perfect Numbers

Mersenne numbers can be used to identify perfect numbers [13]. Thus, Euclid proved that $2^{p-1}\left(2^p-1\right)$ is perfect when 2^p-1 is a prime. Since

$$2^p-1=1+\sum_{j=1}^{p-1}2^j,$$

the divisors of

$$N=2^{p-1}\left(2^p-1\right)$$

are 2^n and $2^n\left(2^p-1\right)$ for n=0,1,2,…,(p-1). For example, with p=3, N=28, and the divisors, including N are 1x7,2x7, and 4x7, so that N=1+2+4+7+14=28, with $M_p=7$.

6. Final Comments

A huge amount of effort has gone into determining the prime factors of Fermat numbers (Table 4) [12]. To reduce the workload, Legendre's Theorem has been used.

Further gains can be made by using integer structure analyses: when the factor $p\in\overline{2}_6$, the factors have the form(64k+1) with k=4+3t, and when $p\in\overline{4}_6$, the factors have the form (64k+1) with k=3t; t=0,1,2,3,… Moreover, the Class of the factors must be consistent with this since $F_n\in\overline{2}_6$. For instance, for F_5, the factor $641\in\overline{2}_6$ and the second factor is in $\overline{4}_6$, thus $\overline{2}_6\overline{4}_6\to\overline{2}_6$. One cannot have $\overline{2}_6\overline{2}_6\to\overline{4}_6$ or $\overline{4}_6\overline{4}_6\to\overline{4}_6$ or $\overline{2}_6\overline{2}_6\overline{4}_6\to\overline{4}_6$ and so on (Table 6).

n	No. of prime factors	p_1^*	row	p_2	row	p_3	row
5	2	$\overline{2}_6$	odd	$\overline{4}_6$	even		
6	2	$\overline{4}_6$	even	$\overline{2}_6$	odd		
7	2	$\overline{2}_6$	odd	$\overline{4}_6$	even		
8	2	$\overline{2}_6$	odd	$\overline{4}_6$	even		
9	3	$\overline{2}_6$	odd	$\overline{2}_6$	odd	$\overline{2}_6$	odd

Table 6: Integer structure analyses (* smallest factor)

To obtain the smallest factor, *pN* may be used so that only $\bar{2}_6\bar{4}_6$ or $\bar{4}_6\bar{2}_6$ need to be considered. For $\bar{2}_6\bar{4}_6$, using $(4+3t_1)$ and $3t_2$ for k_1, k_2, we get:

$$F_n = \left(2^6(4+3t_1)+1\right)\left(2^6(3t_2)+1\right) \tag{6.1}$$

$$2^{2^n} = 2^6\left(2^2+3(t_1+t_2)+3\times 2^8 t_2+9\times 2^6 t_1 t_2\right). \tag{6.2}$$

Since $p \in \bar{2}_6$ (odd row) means $p \in \bar{1}_4 \subset Z_4$ and $p \in \bar{4}_6$ (even row) $\in \bar{1}_4$ too, these primes can be sums of squares [8]. For example,

$$F_5 : p_1 = 641 = 4^2 + 25^2,$$

$$F_9 : p_1 = 2424833 = 127^2 + 1552^2.$$

The workload can also be reduced, of course, with the use of computer algebra systems [4], but we have chosen the approach of this paper so that more of the underlying structure is exposed.

References

1. Krassimir T Atanassov, A Relation between the Prime and the Fibonacci Numbers, *Advanced Studies in Contemporary Mathematics*, **6(1)** (2003): 53-56.
2. John Brillhart, D.H. Lehmer, J.L. Selfridge, Bryant Tuckerman & S.S. Wagstaff Jr, *Factorization of $b^n \pm 1$, b=2,3,5,6,7,10,11,12 up to High Powers. 2nd Edition*. Providence, RI: American Mathematical Society, 1988.
3. Graeme L. Cohen, On a Conjecture of Mąkowski and Schinzel. *Colloquium Mathematicum*, **74(1)** (1997): 1-8.
4. B. Ghusayni, Maple Explorations, Perfect Numbers, and Mersenne Primes. *International Journal of Mathematical Education in Science and Technology*,**36 (6)** (2005): 643-654.
5. G.H. Hardy & E.M. Wright, *An Introduction to the Theory of Numbers*. Oxford: Clarendon Press, 1945, p.14.
6. J.V. Leyendekkers, J.M. Rybak & A.G. Shannon, Integer Class Properties Associated with an Integer Matrix. *Notes on Number Theory & Discrete Mathematics*. **1 (2)** (1995): 53-59.
7. J.V. Leyendekkers, J.M. Rybak & A.G. Shannon, Analysis of Diophantine Properties Using Modular Rings with Four and Six Classes. *Notes on Number Theory & Discrete Mathematics*. **3 (2)** (1997): 61-74.
8. J.V. Leyendekkers, J.M. Rybak & A.G. Shannon, The Characteristics of Primes and Other Integers within the Modular Ring Z_4 and in Class $\bar{1}_4$. *Notes on Number Theory & Discrete Mathematics*. **4 (1)** (1998): 1-17.
9. J.V. Leyendekkers & A.G. Shannon, Expansion of Integer Powers from Fibonacci's Odd Number Triangle. *Notes on Number Theory & Discrete Mathematics*. **7(2)** 2001: 48-59.
10. J.V. Leyendekkers & A.G. Shannon, The Analysis of Twin Primes within Z_6. *Notes on Number Theory & Discrete Mathematics*. **7(4)** 2001: 115-124.

11. J.V. Leyendekkers & A.G. Shannon, Fermat's Theorem on Binary Powers, *Notes on Number Theory & Discrete Mathematics*. Vol. 11, 2005, No. 2, 13-22..
12. Hans Riesel. *Prime Numbers and Computer Methods for Factorization*. 2nd edition. Progress in Mathematics, Volume 126. Boston: Birkhäuser, 1994.
13. W.W. Rouse Ball (revised by H.S.M. Coxeter), *Mathematical Recreations and Essays. 11th Edition*. London: Macmillan, 1956.

AMS Classification Numbers: 11A41, 11A07