NNTDM 11 (2005) 2, 13-22

FERMAT'S THEOREM ON BINARY POWERS

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

Modular rings are used to analyse integers of the form $N = 2^m + 1$. When m is odd, the integer structure prevents the formation of primes. When m is even, N 'commonly' has a right-end-digit of 5 and so is not a prime then. However, a sequence defined by m=4+4q, q=0,1,2,3, can generate some primes as the right-end-digit is 7. Elements of this sequence satisfy the non-linear recurrence relation $G_m = G_{m-1}^2 - 2G_{m-1} + 2$. Fermat numbers, where $m = 2^n$ satisfy this recurrence relation. However, in this case, the integer structure reveals that primes are limited to n<5.

1. Introduction

Around 1640, Fermat claimed that all numbers of the form $2^m + 1$, where $m = 2^n$, are primes [3]. In 1732, Euler showed that when n=5 a composite is formed [2]. Here we shall use the modular rings Z_4 and Z_6 to analyse integers of the form

$$N = 2^m + 1 \tag{1.1}$$

in which m may have any integer value. When m is odd, the integer structure reveals that no primes can be formed; when m is even, we get a more complex result.

Our approach is distinctive and it can, in a sense, be justified by invoking Hoffman's "theory of theories", namely, "a theory will be accepted by a scientific community if it explains better (or more of) what is known, fits at its fringes with what is known about other parts of our universe and makes verifiable, probably risky, predictions"[4].

2. Modular Rings

These have been discussed in detail elsewhere [5,6] so that only a summary is given here.

$\underline{Z_4}$: Integers in this ring have the form $(4r_i + 1)$, with the class represented by $\bar{i}_4$. Even integers $\in \{\bar{0}_4, \bar{2}_4\}$, the latter class having no powers. Odd integers $\in \{\bar{1}_4, \bar{3}_4\}$, the latter class having no even powers, while integers in the former class equal a sum of squares.

$\underline{Z_6}$: Integers in this ring have the form $(6r_i + (i-3))$, with the class represented by $\bar{i}_6$ (Table 1). When 3|*N*, integers $\in \{\bar{3}_6 (even\, N), \bar{6}_6 (odd\, N)\}$. There are no even powers in $\bar{5}_6$ (even *N*) or in $\bar{2}_6$ (odd *N*). Any odd *N* that equals a sum of squares is found in $\bar{2}_6$ ($6r_2 - 1, with\, r_2\, odd$) and in $\bar{4}_6$ ($6r_4 + 1, with\, r_4\, even$).

Class → Row ↓	$\bar{1}_6$	$\bar{2}_6$	$\bar{3}_6$	$\bar{4}_6$	$\bar{5}_6$	$\bar{6}_6$
0	-2	-1	0	1	2	3
1	4	5	6	7	8	9
2	10	11	12	13	14	15
3	16	17	18	19	20	21
4	22	23	24	25	26	27
5	28	29	30	31	32	33
6	34	35	36	37	38	39

Table 1: Z_6 Structure

The relationship between Z_4 and Z_6 is summarised in Table 2.

Modular Ring	Class	Row	Class	Row
Z_4	$\bar{1}_4$	r_1	$\bar{3}_4$	r_3
Z_6	$\bar{2}_6$	$r_2 = \frac{1}{3}(2r_1 + 1)$ r_2 *odd*	$\bar{2}_6$	$r_2 = \frac{2}{3}(r_3 + 1)$ r_2 *even*
	$\bar{4}_6$	$r_4 = \frac{2}{3} r_1$ r_4 *even*	$\bar{4}_6$	$r_4 = \frac{1}{3}(2r_3 + 1)$ r_4 *odd*
	$\bar{6}_6$	$r_6 = \frac{1}{3}(2r_1 - 1)$ r_6 *odd or even*	$\bar{6}_6$	$r_6 = \frac{2}{3} r_3$ r_6 *odd or even*

Table 2: Relationship between Z_4 and Z_6

3. *N* as a Function of *m*

(a) *m* odd.

When m is odd, $2^m \in \bar{5}_6 \left(6r_5 + 2, with \left(r_5\right)_j - \left(r_5\right)_{j-1} = \left(2^{j-1}\right)^2\right)$, so that $N \in \bar{6}_6$ (the next Class in Table 1); hence, 3|*N* and *N* can never be prime.

(b) *m* even; $m \neq 2^n$.

In this case, $2^m \in \bar{1}_6$, so that $N \in \bar{2}_6 \left(6r_2 - 1\right)$. If we consider the right-end-digits (REDs, indicated by an asterisk superscript), then when

$$\left(2^m\right)^* = 4,$$
$$\left(2^m + 1\right)^* = 5,$$

So that except for *m*=2, all such integers will be composite. Furthermore,

$$\left(2^m\right)^* = 6$$

occurs and *N**=7 which could indicate a prime or a composite.

In Z_4, $N = \bar{0}_4 + \bar{1}_4 = \bar{1}_4$, so that $N \in \bar{1}_4$.

In Z_6, only Class $\bar{1}_6$ contains even powers (for even integers), and $3 \nmid N$, so that $N \in \bar{2}_6$ and the row in Table 2 must be odd. Thus $r_2^* = 3$ when $\left(2^m\right)^* = 6$.

These integers can be in either of two series like the Fermat numbers. The principal series has *m*=4+4*q*, but the sub-series is given by

$$m_j = 2m_{j-1}. \tag{3.1}$$

For example, the Fermat numbers obviously satisfy (3.1)

Series where

$$m_j = a \times 2^{j-1}$$

satisfy

$$X_{m_j} = X_{m_{j-1}}^2 - 2X_{m_{j-1}} + 2. \tag{3.2}$$

For example, for

$$\left\{F_m : m_j = 1 \times 2^{j-1}\right\},$$
$$\left\{G_m : m_j = 12 \times 2^{j-1}\right\},$$
$$\left\{H_m : m_j = 20 \times 2^{j-1}\right\},$$

we have

$$\left(2^{a \times 2^{j-1}} + 1\right)^2 - 2\left(2^{a \times 2^{j-1}} + 1\right) + 2 = 2^{a \times 2^j} + 1.$$

These types of integers, when composite, have factors of the form

$$\left(N_1 \times 2^{\omega} + 1\right)\left(N_2 \times 2^{\omega} + 1\right).$$

For example, for $\{G_m\}, m_1 = 12,$

$$\begin{aligned} N &= 2^{12} + 1 (= 4097) \\ &= 2^4(2^8) + 1 \\ &= 2^4(15 \times 2^4 + 1 \times 2^4) + 1 \\ &= (1 \times 2^4 + 1)(15 \times 2^4 + 1) = (17 \times 241); \end{aligned}$$

or, with $m_2 = 24,$

$$\begin{aligned} N &= 2^{24} + 1 (= 16777217) \\ &= 2^5(2^{19}) + 1 \\ &= 2^5(2^{14} \times 2^5) + 1 \\ &= 2^5(16384 \times 2^5) + 1 \\ &= 2^5(3 \times 5 \times 1081 \times 2^5 + 169 \times 2^5) + 1 \\ &= \left(3 \times 2^5 + 1\right)\left(5405 \times 2^5 + 1\right) \\ &(= 97 \times 172961). \end{aligned}$$

In general then, with two factors,

$$\begin{aligned} N &= \left(N_1 2^{\omega} + 1\right)\left(N_2 2^{\omega} + 1\right) \\ &= 2^{\omega}\left(N_1 N_2 2^{\omega} + \left(N_1 + N_2\right)\right) + 1 \\ &= 2^{2\omega}\left(N_1 N_2 + \left(N_1 + N_2\right)2^{-\omega}\right) + 1 \\ &= 2^{2\omega}\left(2^{m-2\omega}\right) + 1, \end{aligned} \tag{3.5}$$

where

$$2^{m-2\omega} = N_1 N_2 + \left(N_1 + N_2\right)2^{-\omega}. \tag{3.6}$$

These relationships will be discussed in more detail in Section 4.

(c) m even; $m = 2^n$.

In the Fermat series, $m = 2^n$, so that

$$F_n = F_{n-1}^2 - 2F_{n-1} + 2. \tag{3.7}$$

3. Factor Structure

$F_n \in \bar{1}_4 \subset Z_4$, $F_n \in \bar{2}_6 \subset Z_6$ so that from Section 3(b):

$$F_n = \left(N_1 2^{\omega} + 1\right)\left(N_2 2^{\omega} + 1\right) \tag{4.1}$$

so that

$$\begin{aligned} F_5 &= \left(5 \times 2^7 + 1\right)\left(3 \times 17449 \times 2^7 + 1\right) \\ &= 2^{14}\left(15 \times 17449 + 409\right) + 1 \\ &= 2^{14}\left(262144\right) + 1 \\ &= 2^{32} + 1; \end{aligned}$$

and

$$\begin{aligned} F_6 &= \left(3 \times 357 \times 2^8 + 1\right)\left(262814145745 \times 2^8 + 1\right) \\ &= 2^{16}\left(3 \times 357 \times 5 \times 52562829149 + 1026617761\right) + 1 \\ &= 2^{16}\left(281474976710656\right) + 1 \\ &= 2^{64} + 1. \end{aligned}$$

On the other hand, suppose

$$F_4 = \left(N_1 2^{\omega} + 1\right)\left(N_2 2^{\omega} + 1\right),\ \omega \in \{6,7\}.$$

When $\omega = 6$,

$$\begin{aligned} F_4 &= 2^6\left(N_1 N_2 \times 2^6 + N_1 + N_2\right) + 1 \\ &= 2^{12}\left(N_1 N_2 + N_3\right) + 1 \end{aligned}$$

and so

$$N_1 N_2 + N_3 = 2^4.$$

Obviously, $N_1 N_2, N_3 < 16$ and are all odd, and $\left(N_1 + N_2\right) \geq 64$, so that the $f\left(N_1, N_2\right)$ cannot fit F_4 which is, in fact, a prime. In Table 3, $\omega \in \{n+2, n+3; n \neq 9,15\}$.

N	**Some factors of Fermat numbers**
9	$\left(37 \times 2^{16} + 1\right)$
11	$\left(39 \times 2^{13} + 1\right)\left(119 \times 2^{13} + 1\right)$
12	$\left(7 \times 2^{14} + 1\right)\left(397 \times 2^{16} + 1\right)\left(973 \times 2^{16} + 1\right)$
15	$\left(579 \times 2^{21} + 1\right)$
18	$\left(13 \times 2^{20} + 1\right)$
23	$\left(5 \times 2^{25} + 1\right)$
36	$\left(5 \times 2^{39} + 1\right)$
8	$\left(3 \times 2^{41} + 1\right)$
73	$\left(5 \times 2^{75} + 1\right)$

Table 3: Some factors of Fermat Numbers

5. Rows of Composites in Z_6

When $N \in Z_6 \left(\supset F_n\right)$ the row R_2 is given by [8,9]:

$$R_2 = R^{'} + pt. \tag{5.1}$$

t=0,1,2,3,…,p is the smallest factor of N and

$$R^{'} = \tfrac{1}{3}\left(\tfrac{1}{2}\left(p^2+1\right)+ p\right),\ p \in \overline{2}_6,$$

or

$$R^{'} = \tfrac{1}{3}\left(\tfrac{1}{2}\left(p^2+1\right)+ 2p\right),\ p \in \overline{4}_6,$$

with

$$\begin{aligned} F_n &= 2^{2^n}+1 \\ &= 6r_2 - 1, \\ r_2 &= \tfrac{1}{3}\left(2^{2^n-1}+1\right), \end{aligned}$$

and, as noted above,

$$r_2^* = 3,\ F_n^* = 7.$$

When F_n is composite,

$$r_2 = R_2,$$

so that

$$2^{2^n-1}+1 = \tfrac{1}{2}\left(p^2+1\right)+ kp + 3pt, \tag{5.2}$$

with k=1 or 2 depending on the class of p.
With

$$F_n = pM,$$

p being the smallest factor,

$$t = \tfrac{1}{6}\left(M - p - 2k\right).$$

Obviously, M>(p+2) or (p+4) for positive t. The range of permissible p increases sharply as F_n increases (Table 4), so that t integer is more achievable as n increases.

n	Limit of prime range
1	-
2	3
3	13
4	257
5	65537
6	4294967307

Table 4: Prime range limits for F_n factors

p*	k	t*
1	1 2	4,9 2,7
3	1 2	4,9 2,7
7	1 2	2,7 0,5
9	1 2	2,7 0,5

Table 5: The RED characteristics

For n=5, the smallest factor is 641, and M=6700417. Since 641=(6x107-1), $p \in \bar{2}_6$ and k=1; thus

$$t = \tfrac{1}{6}\left(6700417 - 641 - 2\right)$$
$$= 1116629,$$

whereas, for n=6, the smallest factor is 274177=(6x45696+1), so $p \in \bar{4}_6$ and k=2. This yields t=11213403506090.

6. Sums of Squares

Fermat proposed, and Euler proved, that a prime, p, which satisfies

$$p = 4r_1 + 1 \tag{6.1}$$

is a sum of squares:

$$p = x^2 + y^2 \tag{6.2}$$

in which (x,y) is unique. This result follows very simply from the integer structure.
In Z_4, only $\bar{0}_4 \subset Z_4$ contains powers of even integers and only $\bar{1}_4 \subset Z_4$ contains even powers of odd integers. Hence with x odd and y even

$$p = \bar{1}_4 + \bar{0}_4 = \bar{1}_4, \tag{6.3}$$

so that $\bar{3}_4$ primes can never be a sum of squares.
The uniqueness of these square pairs has been shown previously [9]. Composites can also have a unique (x,y) pair but in this case x and y have a common factor.
In Z_6, the $\bar{1}_4$ primes appear in both $\bar{2}_6$ and $\bar{4}_6$, but they are identified by the parity of the rows (Table 2). Since $F_n \in \left\{\bar{1}_4, \bar{2}_6\right\}$ (with odd row)

$$F_n = x^2 + y^2. \tag{6.4}$$

When F_n is prime the (x,y) couple is unique as noted above. All F_n have the (x,y) couple $\left(1,2^{2^{n-1}}\right)$ and as F_n increases, the probability of finding a value for x, other than 1, increases greatly (Table 6).

n	$F_n - 1$	**(*x*,*y*)**
1	4	(1,2)
2	16	(1,4)
3	256	(1,16)
4	65536	(1,256)
5	4294967296	(1,65536)
		(20449,62264)

Table 6: (x,y) pairs

7. Final Comments

Fermat's numbers belong to a subgroup where $N = 2^m + 1$, with m even. This subgroup has the lowest initial values for m (1,2,4,8,16) which permits primes to be formed; (m=12 is the starter for another group, (all composites)). The general series with m=4+4q (q=0,1,2,3,…) is essentially a composite-forming series, and Fermat's assumption of prime generation is only true for lowest m. The factors of the general series have the form $N \times 2^{\omega} + 1$ as shown in Table 3 for the Fermat numbers. Generally $\omega \in \{n+2, n+3\}$: it would be of interest to determine why these values apply.

Composite status can be investigated from the characteristic row functions for composites. All $F_n \in \bar{1}_4$ which is equivalent to $\bar{2}_6$ with odd row. Hence F_n equals a sum of squares $\left(x^2 + y^2\right)$ in which x is always unity for primes; when F_n is composite, x has other values as well, the number of such values depending on the number of factors. (The values of y change accordingly.)
Since

$$F_n = \begin{cases} F_{n-1}^2 - 2F_{n-1} + 2 & or \\ F_0F_1F_2F_3...F_{n-1} + 2. \end{cases}$$

the factors may be described by F_n functions. For example,

$$F_5 = \left(\tfrac{1}{2}\left(F_1F_3 - F_0\right)\right)\left(F_0\left(\left(F_3 - 1\right)\left(2F_2F_3 - \tfrac{1}{2}F_0^3\right)\right) + 1\right). \tag{7.1}$$

A sum may also represent $2^m + 1$, that is

$$2^m + 1 = 3 + \sum_{j=1}^{m-1} 2^j,\ m \geq 1. \tag{7.2}$$

According to Pepin's Theorem [10], a necessary and sufficient condition for

$$F_n = 2^{2^n} + 1,\ n \geq 1,$$

to be a prime is that

$$3^{2^{2n-1}} \equiv -1 \pmod{F_n}. \tag{7.3}$$

This theorem has been used to test the primality of F_n up to n=22. All values are composite when n>4. (See Table 4 in [11] for a list of prime factors of Fermat numbers.) We note in conclusion though that we are primarily expounding another theoretical insight into an old problem in contrast to the more fashionable computational approaches. In the words of Odifreddi [10]: "As is often the case with technology, many changes are for the worse, and the mathematical applications of the computer are no exception. Such is, for example, the case when the computer is used as an *idiot savant*, in the anxious and futile search for ever larger prime numbers"!

Conway and Guy [1] consider Fermat numbers to the base 10 as well as to the base 2. They also mention that Gauss proved "the surprising fact that if p is a Fermat prime, then a regular polygon with p sides can be constructed with ruler and compass, using Euclid's rules… It's said that Gauss requested that a regular 17-gon be inscribed on his tombstone. This wasn't done, but there is a regular 17-gon on a monument to Gauss in Braunschweig" (the location of the 11th International Research Conference on Fibonacci Numbers and Their Applications in 2004).

References

1. John H Conway & Richard K Guy, *The Book of Numbers*. New York: Copernicus, 1996.
2. L. Euler, *Opera Omnia*. Leipzig: Teubner, 1911.
3. G.H. Hardy & E.M. Wright, *An Introduction to the Theory of Numbers*. 3rd edition. London & New York: Oxford University Press, 1954.
4. Roald Hoffmann. Why Buy That Theory? *American Scientist*, **91(1)** (2003): 9-11.
5. 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.
6. 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.
7. 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.
8. 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.

9. J.V. Leyendekkers & A.G. Shannon, Using Integer Structure to Count the Number of Primes in a Given Interval, *Notes on Number Theory & Discrete Mathematics*. In press.
10. Piergiorgio Odifreddi. *The Mathematical Century*. (Translated by Arturo Sangalli; foreword by Freeman Dyson.) Princeton: Princeton University Press, 2004.
11. Hans Riesel. *Prime Numbers and Computer Methods for Factorization*. 2nd edition. Progress in Mathematics, Volume 126. Boston: Birkhäuser, 1994.

AMS Classification Numbers: 11A41, 11A07