NNTDM 13 (2007), 3, 27-35

MODULAR-RING CLASS STRUCTURES OF $x^n \pm y^n$

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

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

Abstract

Integer structure theory is used to analyse the factors of sums and differences of two identical powers of two integers, *x* and *y*. For instance, the sum of two identical powers, *m*, cannot form primes when *m* is odd or when *m* is even if the powers are odd and of the form $m/2^n$. The expanded forms of the factors indicate why the structure acts against the sum ever equalling an identical power. The difference of odd powers can yield primes when $x - y = 1$ The difference of even powers cannot yield primes whereas the sum can when $m/2^n$ is even. However, $x^2 - y^2$ can equal a prime when $x - y = 1$.

1. Introduction

This paper is an extension of "two-squares" identities which go back at least to the early thirteenth century [4] or possibly earlier still [2]. Craig [1] provides a convenient summary of such identities and applies group-theoretic tools to binary quadratic decomposition. Here we build on a previous note [3], to the effect that $\left(x^n + y^n\right)$, n>1 and odd, can never be a prime since

$$\begin{aligned} x^n + y^n &= \left(x + y\right)\left(x^{n-1} + y^{n-1} - \frac{xy}{x+y}\left(x^{n-2} + y^{n-2}\right)\right) \\ &= \left(x+y\right)f\left(x,y\right) \end{aligned} \tag{1.1}$$

nor can $\left(x^n - y^n\right)$ produce primes since

$$\begin{aligned} x^n - y^n &= \left(x - y\right)\left(x^{n-1} + y^{n-1} + \frac{xy}{x-y}\left(x^{n-2} - y^{n-2}\right)\right) \\ &= \left(x-y\right)g\left(x,y\right) \end{aligned} \tag{1.2}$$

except in (1.2) when x=2 and y=1 or x-y=1 when primes can be formed. In the former case $\left(x^n - y^n\right)$ becomes $\left(2^n - 1\right)$ which is a Mersenne number when n is prime.

If the exponent, m say, is even and $(m/2^n)$ is odd, then on replacing x and y by x^{2^n} and y^{2^n} respectively, and n by $m/2^n$, we can use Equations (1.1) and (1.2) in the form

$$\left(x^{2^n}\right)^{m/2^n} + \left(y^{2^n}\right)^{m/2^n} = x^m + y^m. \tag{1.3}$$

Thus, with the exceptions noted, primes can only be formed from the sum of two powers, m, when m is a power of 2 such as $x^4 + y^4$ [3]. In this paper we explore the class structure of the factors of the three types of non-prime forming triples, using the modular ring Z_4 (Table 1).

2. $x^n + y^n, n$ odd

Relationship of (x+y) and f(x,y)

For low prime values, when (x+y) is a prime, f(x,y) is also a prime. However the integer structure shows that this is not a general rule. For example, let n=3 and x=4 and y=19, so that from $Z_4, x = 4r_0\ (r_0 = 1)$ and $y = 4r_3 + 3(r_3 = 4)$, thus

$$(x+y) \quad = 4(r_0 + r_3) + 3 = 23, \tag{2.1}$$

$$\begin{aligned} f(x,y) \quad &= x^2 + y^2 - xy \\ &= 16\left(r_0^2 + r_3^2 - r_0 r_3\right) + 12(2r_3 - r_0) + 9. \end{aligned} \tag{2.2}$$

Row $(r_i)\downarrow$ Class (i)→	$\bar{0}_4$	$\bar{1}_4$	$\bar{2}_4$	$\bar{3}_4$	Comments
0	0	1	2	3	$N = 4r_i + i$
1	4	5	6	7	even $\bar{0}_4, \bar{2}_4$
2	8	9	10	11	$\left(N^n, N^{2n}\right) \in \bar{0}_4$
3	12	13	14	15	odd $\bar{1}_4, \bar{3}_4; N^{2n} \in \bar{1}_4$

Table 1: Rows and classes for Z_4

If $f(x,y)$ is a prime then the right hand side of Equation (2.2) has no prime factors. However, 7 is a common factor of $\left(16\left(r_0^2 + r_3^2 - r_0 r_3\right) + 9\right)$ and $\left(12(2r_3 - r_0)\right)$. Obviously, the various combinations of the rows indicate, even for this small n, that a common factor could be easily obtained. In general, when (x+y) = nk, k odd,

$$x^n + y^n = n^2 k\left(f(n,k,y) + y^{n-1}\right). \tag{2.3}$$

Table 2 shows some examples which illustrate how difficult a resultant of z^n would be.

n	$(x+y)$	$(x+y)\left(x^{n-1}+y^{n-1}-\frac{xy}{x+y}\left(x^{n-2}+y^{n-2}\right)\right)$
3	$3k$	$3^2k\left(3k^2-3ky+y^2\right)$
5	$5k$	$5^2k\left(5^3k^4-5^3k^3y+5\times 34k^2y^2-10ky^3+y^4\right)$
3	Nk	$Nk\left(N^2k^2-3Nky+3y^2\right)$

Table 2: When $n\,|\,(x+y)$, then $n\,|\,f(x,y)$

The same applies when $(x+y) = Nk$ with $N \neq n$ (Table 2). In this case,

$$x^n + y^n = Nk\left(f(N,k,y)+ny^{n-1}\right). \tag{2.4}$$

If

$$\left(f(N,k,y)+ny^{n-1}\right)=(Nk)^{n-1}, \tag{2.5}$$

then

$$y = Nk.$$

But

$$x+y = Nk,$$

so that

$$x^n + y^n \neq (Nk)^n. \tag{2.6}$$

If

$$\left(f(N,k,y)+ny^{n-1}\right)=A^n(Nk)^{n-1},$$

Then y cannot have an integer solution so that the inequation (2.6) applies again with $A^n(Nk)^{n-1}$ on the right hand side. The same argument can be applied over and over again.

Class Structure

If we take x even and y odd, then we can deduce the class of $\left(x^n+y^n\right)$(Table 3). For n=3, when $y\in\bar{3}_4, \left(x^3+y^3\right)$can never equal a sum of squares, whereas when $y\in\bar{1}_4$, the sum of cubes can equal a sum of squares.

Number	**Classes**					
	x	y	x+y	x^2+y^2-xy	$(x+y)f(x,y)=N$	Comments
1	$\bar{2}_4$	$\bar{1}_4$	$\bar{3}_4$	$\bar{0}_4+\bar{1}_4-\bar{2}_4=\bar{3}_4$	$\left(\bar{3}_4\times\bar{3}_4\right)\in\bar{1}_4$	$N=a^2+b^2$
2	$\bar{2}_4$	$\bar{3}_4$	$\bar{1}_4$	$\bar{0}_4+\bar{1}_4-\bar{2}_4=\bar{3}_4$	$\left(\bar{1}_4\times\bar{3}_4\right)\in\bar{3}_4$	$N\neq a^2+b^2$
3	$\bar{0}_4$	$\bar{1}_4$	$\bar{1}_4$	$\bar{0}_4+\bar{1}_4-\bar{0}_4=\bar{1}_4$	$\left(\bar{1}_4\times\bar{1}_4\right)\in\bar{1}_4$	$N=a^2+b^2$
4	$\bar{0}_4$	$\bar{3}_4$	$\bar{3}_4$	$\bar{0}_4+\bar{1}_4-\bar{0}_4=\bar{1}_4$	$\left(\bar{3}_4\times\bar{1}_4\right)\in\bar{3}_4$	$N\neq a^2+b^2$

Table 3(a): Class structure in Z_4 when n=3

Number	Classes		$(x+y)(x^6+y^6)$	$xy(x^5+y^5)$	
	x	y	a	b	N=a-b
1	$\bar{2}_4$	$\bar{1}_4$	$\bar{3}_4 \times (\bar{0}_4 + \bar{1}_4) = \bar{3}_4$	$\bar{2}_4 \times \bar{1}_4 (\bar{0}_4 + \bar{1}_4) = \bar{2}_4$	$\bar{1}_4$
2	$\bar{2}_4$	$\bar{3}_4$	$\bar{1}_4 \times (\bar{0}_4 + \bar{3}_4) = \bar{3}_4$	$\bar{2}_4 \times \bar{1}_4 (\bar{0}_4 + \bar{3}_4) = \bar{2}_4$	$\bar{1}_4$
3	$\bar{0}_4$	$\bar{1}_4$	$\bar{1}_4 \times (\bar{0}_4 + \bar{1}_4) = \bar{1}_4$	$\bar{0}_4 \times \bar{1}_4 (\bar{0}_4 + \bar{1}_4) = \bar{0}_4$	$\bar{1}_4$
4	$\bar{0}_4$	$\bar{3}_4$	$\bar{3}_4 \times (\bar{0}_4 + \bar{3}_4) = \bar{1}_4$	$\bar{0}_4 \times \bar{3}_4 (\bar{0}_4 + \bar{3}_4) = \bar{0}_4$	$\bar{1}_4$

Table 3(b): Class structure in Z_4 when n=7

However, when n>3 the sum of the two powers always falls in Class $\bar{1}_4$ (Table 3(b)) so that the power sum equals a sum of squares. Furthermore, when n>3 and there are factors in Class $\bar{3}_4$, there must be an even number of such factors since $(\bar{3}_4 \times \bar{1}_4) \in \bar{3}_4$, $(\bar{3}_4 \times \bar{3}_4) \in \bar{1}_4$, $\bar{3} \times (\bar{3}_4 \times \bar{3}_4) \in \bar{3}_4$, and so on. In turn, this means that since such factors are to an even power, they cannot give the odd power required if $x^n + y^n = z^n$, which is consistent with Fermat's Last Theorem. The manner in which factors arise can be understood by using the class functions. Some examples for n=3 are shown in Table 4.

No*	*x*+*y*	*f*(*x*,*y*)	Examples
1	$4(r_1 + r_2) + 3 \in \bar{3}_4$	$16(r_2^2 + r_2 + r_1^2 - r_1 r_2)$ $-4r_2 + 3 \in \bar{3}_4$	$x = 2,\ y = 13:$ $x \in \bar{2}_4,\ r_2 = 0,$ $y \in \bar{1}_4,\ r_1 = 3;$ $f((x,y) = 16 \times 9 + 3$ $= 3 \times 7^2$
2	$4(r_2 + r_3 + 1) + 1 \in \bar{1}_4$	$16(r_2^2 + r_2 + r_3^2 - r_2 r_3)$ $+4(4r_3 - 3r_2) + 7 \in \bar{3}_4$	(a) x=2; y=23: $x \in \bar{2}_4, r_2 = 0,$ $y \in \bar{3}_4, r_3 = 5;$ $f(x,y) = 16 \times 25 + 4 \times 20 + 7$ no prime factors; so prime. (b) x=6; y=11: $x \in \bar{2}_4, r_2 = 1,$ $y \in \bar{3}_4, r_3 = 2;$ $f(x,y) = 16 \times 4 + 4 \times 5 + 7$ $= 7 \times 13.$
3	$4(r_0 + r_1) + 1 \in \bar{1}_4$	$16(r_0^2 + r_1^2 - r_0 r_1)$ $+4(2r_1 - r_0) + 1 \in \bar{1}_4$	(a) x=4; y=17:

			$x \in \bar{0}_4, r_0 = 1,$ $y \in \bar{1}_4, r_1 = 4;$ $f(x,y) = 16\times 13 + 28 + 1$ $= 3\times 79.$ (b) x=4; y=13: $x \in \bar{0}_4, r_0 = 1,$ $y \in \bar{1}_4, r_1 = 3;$ $f(x,y) = 16\times 7 + 20 + 1$ $= 7\times 19..$
4	$4(r_0 + r_3) + 3 \in \bar{3}_4$	$16(r_0^2 + r_3^2 - r_2 r_3)$ $+4(6r_3 - 3r_0) + 9 \in \bar{1}_4$	(a) x=4; y=19: $x \in \bar{0}_4, r_0 = 1,$ $y \in \bar{3}_4, r_3 = 4;$ $f(x,y) = 16\times 13 + 12\times 7 + 9$ $= 7\times 43.$ (b) x=24; y=19: $x \in \bar{0}_4, r_0 = 6,$ $y \in \bar{3}_4, r_3 = 4;$ $f(x,y) = 16\times 28 + 7 + 26$ $= 13\times 37.$

Table 4: Formation of factors for n=3 (* from Table 2)

3. $x^n - y^n$, *n* odd

As for $x^n + y^n$, we can deduce the class of $x^n - y^n$, (Table 5).

Number	**Classes**				
	x	y	x-y	g(x,y)	$(x-y)g(x,y) = N$
1	$\bar{2}_4$	$\bar{1}_4$	$\bar{1}_4$	$\bar{0}_4 + \bar{1}_4 + \bar{2}_4 = \bar{3}_4$	$(\bar{1}_4 \times \bar{3}_4) \in \bar{3}_4$
2	$\bar{2}_4$	$\bar{3}_4$	$\bar{3}_4$	$\bar{0}_4 + \bar{1}_4 + \bar{2}_4 = \bar{3}_4$	$(\bar{3}_4 \times \bar{3}_4) \in \bar{1}_4$
3	$\bar{0}_4$	$\bar{1}_4$	$\bar{3}_4$	$\bar{0}_4 + \bar{1}_4 + \bar{0}_4 = \bar{1}_4$	$(\bar{3}_4 \times \bar{1}_4) \in \bar{3}_4$
4	$\bar{0}_4$	$\bar{3}_4$	$\bar{1}_4$	$\bar{0}_4 + \bar{1}_4 + \bar{0}_4 = \bar{1}_4$	$(\bar{1}_4 \times \bar{1}_4) \in \bar{1}_4$

Table 5(a): Class structure in Z_4 when n=3

When $y \in \bar{3}_4, (x^n - y^n) \in \bar{1}_4$ and hence equal to a sum of squares.

Number	Classes		$(x-y)(x^4+y^4)$	$xy(x^3-y^3)$	
	x	y	a	b	$N=a+b$
1	$\bar{2}_4$	$\bar{1}_4$	$\bar{1}_4 \times (\bar{0}_4 + \bar{1}_4) = \bar{1}_4$	$\bar{2}_4 \times \bar{1}_4 (\bar{0}_4 - \bar{1}_4) = \bar{2}_4 \times \bar{3}_4 = \bar{2}_4$	$\bar{3}_4$
2	$\bar{2}_4$	$\bar{3}_4$	$\bar{3}_4 \times (\bar{0}_4 + \bar{1}_4) = \bar{3}_4$	$\bar{2}_4 \times \bar{1}_4 (\bar{0}_4 - \bar{3}_4) = \bar{2}_4 \times \bar{1}_4 = \bar{2}_4$	$\bar{1}_4$
3	$\bar{0}_4$	$\bar{1}_4$	$\bar{3}_4 \times (\bar{0}_4 + \bar{1}_4) = \bar{3}_4$	$\bar{0}_4 \times \bar{1}_4 (\bar{0}_4 - \bar{1}_4) = \bar{0}_4 \times \bar{3}_4 = \bar{0}_4$	$\bar{3}_4$
4	$\bar{0}_4$	$\bar{3}_4$	$\bar{1}_4 \times (\bar{0}_4 + \bar{1}_4) = \bar{1}_4$	$\bar{0}_4 \times \bar{3}_4 (\bar{0}_4 - \bar{3}_4) = \bar{0}_4 \times \bar{1}_4 = \bar{0}_4$	$\bar{1}_4$

Table 5(b): Class structure in Z_4 when n=5. (NB: $(\bar{3}_4)^{2n} \in \bar{1}_4$

Unlike $(x^n + y^n)$, the difference of the powers may fall in either $\bar{1}_4$ or $\bar{3}_4$ for all odd powers. When $x \in \bar{2}_4, y \in \bar{3}_4, n = 3,$ the factors are both in $\bar{3}_4$ so, if identical, will produce an even power.

When $n \geq 5,$ the class of $(x^n - y^n)$ and $(x-y)$ yields the $g(x,y)$ class. For example, when $(x - y \in \bar{1}_4)$ and the difference of powers $N \in \bar{3}_4$, then $g(x,y) \in \bar{3}_4$ because $\bar{1}_4 \times \bar{3}_4 = \bar{3}_4$. On the other hand, when $(x - y \in \bar{3}_4)$ and $N \in \bar{3}_4$, then $g(x,y) \in \bar{1}_4$. An analysis of the factor structure can be made as for $x^n + y^n$.

Since $(a-b) \neq (b-a)$ for $a \neq b$, the class structure in this case is not independent of parity and the relative magnitude of x and y. For instance, if we take x odd and y even, $x>y$, then the class structure is reversed (Table 5c).

Number	x	y	$x^3 - y^3$	$x^5 - y^5$
1	$\bar{1}_4$	$\bar{2}_4$	$\bar{1}_4$	$\bar{1}_4$
2	$\bar{3}_4$	$\bar{2}_4$	$\bar{3}_4$	$\bar{3}_4$
3	$\bar{1}_4$	$\bar{0}_4$	$\bar{1}_4$	$\bar{1}_4$
4	$\bar{3}_4$	$\bar{0}_4$	$\bar{3}_4$	$\bar{3}_4$

Table 5(c): Class structure in Z_4 when n=3, 5

4. $x^m \pm y^m, m/2^n$ odd

As noted above, for even indices, m, when $m/2^n$ is odd, the above comments apply since

$$x^m + y^m = \left(x^{2^n}\right)^{\frac{m}{2^n}} + \left(y^{2^n}\right)^{\frac{m}{2^n}} \tag{4.1}$$

so that with

$$X = x^{2^n}, Y = y^{2^n}, q = \tfrac{m}{2^n},$$

$$(x^m + y^m) = (X+Y)\left(X^{q-1} + Y^{q-1} - XY\left(X^{q-2} + Y^{q-2}\right)/(X+Y)\right), \tag{4.2}$$

and

$$\left(x^m - y^m\right) = \left(X - Y\right)\left(X^{q-1} + Y^{q-1} + XY\left(X^{q-2} - Y^{q-2}\right)/\left(X - Y\right)\right). \tag{4.3}$$

For example, when y=n=1, Equation (4.2) becomes

$$\left(x^m + 1\right) = \left(x^2 + 1\right)\left(\left(x^2\right)^{\frac{m}{2}-1} + 1 - x^2\left(\left(x^2\right)^{\frac{m}{2}-2} + 1\right)/\left(x^2 + 1\right)\right), \tag{4.4}$$

or, with *m*=70,

$$\left(x^{70} + 1\right) = \left(x^2 + 1\right)\left(\left(x^2\right)^{34} + 1 - x^2\left(\left(x^2\right)^{33} + 1\right)/\left(x^2 + 1\right)\right), \tag{4.5}$$

Consider *x*=2, *y*=1. For $2^n + 1$ the parity and class of *n* determine the right end digit (RED) of 2^n (Table 6). This information is useful when analysing $2^n + 1$ in functions of Aurifeuilian factors. For example, consider the function $2^m + 1$ and the associated Aurifeuilian factors (Table 7). Since all *m* in the first column are in class $\bar{2}_4$, the RED of $2^m + 1$ will be 5, so that 5 will always be a factor.

n	**Class**	**RED of** $2^n, 2 \in \bar{2}_4$	**RED of** $4^n, 4 \in \bar{0}_4$
even	$\bar{2}_4$	4	6
even	$\bar{0}_4$	6	6
odd	$\bar{1}_4$	2	4
odd	$\bar{3}_4$	8	4

Table 6: Right End Digits (REDs)

$x^m + y^m$	**Aurifeuillian Factors**
$2^6 + 1$	$\left(2^3 - 2^2 + 1\right)\left(2^3 + 2^2 + 1\right)$
$2^{10} + 1$	$\left(2^5 - 2^3 + 1\right)\left(2^5 + 2^3 + 1\right)$
$2^{14} + 1$	$\left(2^7 - 2^4 + 1\right)\left(2^7 + 2^4 + 1\right)$
$2^{30} + 1$	$\left(2^{15} - 2^8 + 1\right)\left(2^{15} + 2^8 + 1\right)$
$2^{42} + 1$	$\left(2^{21} - 2^{11} + 1\right)\left(2^{21} + 2^{11} + 1\right)$
$2^{70} + 1$	$\left(2^{35} - 2^{18} + 1\right)\left(2^{35} + 2^{18} + 1\right)$

Table 7: Aurifeuillian Factors

The first Aurifeuillian Factor has the form $\left(2^s - 2^t + 1\right)$ and the second one has the form $\left(2^s + 2^t + 1\right)$. The REDs of these factors are formed as shown in Table 6 so that the term containing the factor 5 can easily be identified (Table 8). Compare these results with Equation (4.5)

$$2^{70} + 1 = 5\left(4^{34} + 1 - \tfrac{4}{5}\left(4^{33} + 1\right)\right).$$

Since 4 to an odd power always has a RED of 4 (Table 6), $\left(4^{33} + 1\right)$ always has a factor 5.

s	Class	RED of 2^s	t	Class	RED of 2^t	REDs	
						$(2^s - 2^t + 1)^*$	$(2^s + 2^t + 1)^*$
3	$\bar{3}_4$	8	2	$\bar{2}_4$	4	5	3
5	$\bar{1}_4$	2	3	$\bar{3}_4$	8	5	1
7	$\bar{3}_4$	8	4	$\bar{0}_4$	6	3	5
15	$\bar{3}_4$	8	8	$\bar{0}_4$	6	3	5
21	$\bar{1}_4$	2	11	$\bar{3}_4$	8	5	1
35	$\bar{3}_4$	8	18	$\bar{2}_4$	4	5	3

Table 8: REDs of Aurifeuillian Factors

5. $x^m - y^m, m = 2^n, n > 1$

We have

$$x^m - y^m = \left(x^{\frac{m}{2}}\right)^2 - \left(y^{\frac{m}{2}}\right)^2 = \left(x^{\frac{m}{2}} - y^{\frac{m}{2}}\right)\left(x^{\frac{m}{2}} + y^{\frac{m}{2}}\right). \quad (5.1)$$

Obviously for a prime to be present, either factor in (5.1) must be unity. Neither is possible, however, when $x, y > 0$. For example, when $m = 4$, $n = 2$, we need

$$x^2 - y^2 = 1. \quad (5.2)$$

But

$$x^2 - y^2 = (x - y)(x + y) \quad (5.3)$$

so that Equation (5.2) cannot equal 1 when $x, y > 0$. Hence $x^m - y^m, m = 2^n, n > 1$ cannot be a prime because, with that exponent, one can always factor it into a difference of two squares.

We have discussed $x^m + y^m, m = 2^n$ previously [3] and shown that primes can be formed, when the integer structure is compatible. When $n = 2$, many primes can be formed.

A class analysis along the lines of Table 5 will show that $\left(x^{2^n} - y^{2^n}\right) \in \bar{3}_4$ for all n and thus can never equal a sum of squares. However, if x is odd and y even with $x > y$ and the same class analysis is carried out, then it will be found that now all $\left(x^{2^n} - y^{2^n}\right) \in \bar{1}_4$ and thus can equal a sum of squares.

References

1. Craig, Maurice. The Composition Heresies. *The Australian Mathematical Society Gazette.* Vol.33, No.4(2006), 265-272.
2. Dickson, L.E. *History of the Theory of Numbers*. *Volume 3*. New York: Chelsea, 1952.

3. Leyendekkers, J.V., A.G. Shannon, Integer Structure Analysis of Primes and Composites from $(x^4 + y^4)$. *Notes on Number Theory & Discrete Mathematics*. Submitted.
4. Rouse Ball, W.W. *History of Mathematics*. New York: Dover, 1960.

AMS Classification Numbers: 11A41, 11A07